LANCOM 821 ADSL/ISDN –
LANCOM 1621 ADSL/ISDN –
LANCOM 1711 VPN

© 2004 LANCOM Systems GmbH, Würselen (Germany). Alle Rechte vorbehalten.

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Weitergabe und Vervielfältigung der zu diesem Produkt gehörenden Dokumentation und Software und die Verwendung ihres Inhalts sind nur mit schriftlicher Erlaubnis von LANCOM gestattet. Änderungen, die dem technischen Fortschritt dienen, bleiben vorbehalten.

Windows®, Windows NT® und Microsoft® sind eingetragene Marken von Microsoft, Corp.

Das LANCOM-Logo und die Bezeichnung LANCOM sind eingetragene Marken der LANCOM Systems GmbH. Alle übrigen verwendeten Namen und Bezeichnungen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

LANCOM behält sich vor, die genannten Daten ohne Ankündigung zu ändern, und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit http://www.openssl.org/.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom.de

Würselen, Juni 2004

110238/0604

Ein Wort vorab

Vielen Dank für Ihr Vertrauen!

Mit dem LANCOM haben Sie sich für einen leistungsfähigen Router entschieden, der serienmäßig sowohl über integrierte DSL- bzw. ADSL- sowie ISDN-Schnittstellen als auch über einen 4-Port-Switch verfügt. Mit diesem Router schließen Sie einen einzelnen Arbeitsplatzrechner oder ein ganzes lokales Netzwerk einfach und komfortabel ans Highspeed-Internet an.

Sicherheitseinstellungen

Für einen sorglosen Umgang mit Ihrem Produkt empfehlen wir Ihnen, sämtliche Sicherheitseinstellungen (z.B. Firewall, Verschlüsselung, Zugriffsschutz, Gebührensperre) vorzunehmen, die nicht bereits zum Zeitpunkt des Kaufs des Produkts aktiviert waren. Der LANconfig-Assistent 'Sicherheitseinstellungen' unterstützt Sie bei dieser Aufgabe. Weitere Informationen zum Thema Sicherheit finden Sie auch im Kapitel 'Sicherheits-Einstellungen' auf Seite 70.

Zusätzlich bitten wir Sie, sich auf unserer Internet-Seite www.lancom.de über technische Weiterentwicklungen und aktuelle Hinweise zu Ihrem Produkt zu informieren und ggf. neue Software-Versionen herunterzuladen.

Benutzerhandbuch und Referenzhandbuch

Die Dokumentation Ihres Gerätes besteht aus zwei Teilen: Dem Benutzerhandbuch und dem Referenzhandbuch.

Sie lesen derzeit das Benutzerhandbuch. Es enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Das Referenzhandbuch befindet sich als Acrobat-Dokument (PDF-Datei) auf CD. Es ergänzt das Benutzerhandbuch und geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Dazu zählen beispielsweise:

- Systemdesign des Betriebssystems LCOS
- Konfiguration
- Management
- Diagnose
- Sicherheit
- Routing- und WAN-Funktionen
- Firewall
- Quality of Service (QoS)

DE

- Virtuelle Private Netzwerke (VPN)
- Virtuelle lokale Netzwerke (VLAN)
- Funknetzwerke (WLAN)
- LANCAPI
- weitere Server-Dienste (DHCP, DNS, Gebührenmanagement)

Modellvarianten

Das vorliegende Benutzerhandbuch gilt für die folgenden Modelle der LANCOM-Serie:

- LANCOM 821 ADSL/ISDN
- LANCOM 1621 ADSL/ISDN
- LANCOM 1711 VPN

Modell-Einschränkungen

Die Teile der Dokumentation, die nur für ein bestimmtes Modell gelten, sind entweder im Text selbst oder durch entsprechende seitliche Hinweise gekennzeichnet.

In den anderen Teilen der Dokumentation werden alle beschriebenen Modelle unter dem Sammelbegriff LANCOM zusammengefasst.

An der Erstellung dieser Dokumentation …

… haben mehrere Mitarbeiter/innen aus verschiedenen Teilen des Unternehmens mitgewirkt, um Ihnen die bestmögliche Unterstützung bei der Nutzung Ihres LANCOM-Produktes anzubieten.

Sollten Sie einen Fehler finden, oder einfach nur Kritik oder Anregung zu dieser Dokumentation äußern wollen, senden Sie bitte eine E-Mail direkt an:

info@lancom.de

Sollten Sie zu den in diesem Handbuch besprochenen Themen noch Fragen haben oder zusätzliche Hilfe benötigen, steht Ihnen unser Internet-Server www.lancom.de rund um die Uhr zur Verfügung. Hier finden Sie im Bereich 'Support' viele Antworten auf „häufig gestellte Fragen ('FAQs')". Darüber hinaus bietet Ihnen die Wissensdatenbank einen großen Pool an Informationen. Aktuelle Treiber, Firmware, Tools und Dokumentation stehen für Sie jederzeit zum Download bereit.
Außerdem steht Ihnen der LANCOM-Support zur Verfügung. Telefon-

nummern und Kontaktadressen des LANCOM-Supports finden Sie in einem separaten Beileger oder auf der LANCOM-Homepage.

Hinweis-Symbole	
	Sehr wichtiger Hinweis, dessen Nichtbeachtung zu Schäden führen kann.
	Wichtiger Hinweis, der beachtet werden sollte.
	Zusätzliche Informationen, deren Beachtung hilfreich sein kann aber nicht erforderlich ist.

DE

Inhalt

1 Einleitung 9

1.1 Wie funktioniert ADSL? 9

1.2 Welchen Nutzen bietet VPN? 12

1.3 Firewall 15

1.4 Was macht ein Router? 17

1.4.1 Brückenkopf zum WAN 17

1.4.2 Einsatzgebiete für Router 18

1.5 Was kann Ihr LANCOM? 19

2 Installation 22

2.1 Lieferumfang 22

2.2 Systemvoraussetzungen 22

2.3 LANCOM stellt sich vor 23

2.3.1 Statusanzeigen 23

2.3.2 Die Anschlüsse des Geräts 28

2.4 Installation der Hardware 30

2.5 Installation der Software 31

2.5.1 LANCOM-Setup starten 32

2.5.2 Welche Software installieren? 32

3 Grundkonfiguration 34

3.1 Welche Angaben sind notwendig? 34

3.1.1 TCP/IP-Einstellungen 34

3.1.2 Konfigurationsschutz 36

3.1.3 Einstellungen für den DSL-Anschluss 36

3.1.4 Einstellungen für den ISDN-Anschluss 36

3.1.5 Gebührenschutz 37

3.2 Anleitung für LANconfig 37

3.3 Anleitung für WEBconfig 39

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs 44

DE

4 Den Internet-Zugang einrichten 46

4.1 Anleitung für LANconfig 48

4.2 Anleitung für WEBconfig 48

5 Zwei Netzwerke verbinden 50

5.1 Welche Angaben sind notwendig? 51

5.1.1 Allgemeine Angaben 51

5.1.2 Einstellungen für den TCP/IP-Router 53

5.1.3 Einstellungen für den IPX-Router 55

5.1.4 Einstellungen für NetBIOS-Routing 56

5.2 Anleitung für LANconfig 56

5.3 Anleitung für WEBconfig 57

6 Einwahl-Zugang bereitstellen 59

6.1 Welche Angaben sind notwendig? 60

6.1.1 Allgemeine Angaben 60

6.1.2 Einstellungen für TCP/IP 61

6.1.3 Einstellungen für IPX 62

6.1.4 Einstellungen für NetBIOS-Routing 62

6.2 Einstellungen am Einwahl-Rechner 63

6.2.1 Einwahl über VPN 63

6.2.2 Einwahl über ISDN 63

6.3 Anleitung für LANconfig 64

6.4 Anleitung für WEBconfig 65

7 Faxe versenden mit der LANCAPI 66

7.1 Installation des LANCOM CAPI Faxmodem 67

7.2 Installation des MS Windows Faxdienstes 68

7.3 Versenden eines Faxes 68

7.3.1 Faxe versenden mit beliebigen Büroanwendungen 68

7.3.2 Faxe versenden mit dem Windows Faxdienst 69

DE

8 Sicherheits-Einstellungen 70

8.1 Der Sicherheits-Assistent 70
8.1.1 Assistent für LANconfig 70
8.1.2 Assistent für WEBconfig 71

8.2 Der Firewall-Assistent 71
8.2.1 Assistent für LANconfig 72
8.2.2 Konfiguration unter WEBconfig 72

8.3 Die Sicherheits-Checkliste 72

9 Rat & Hilfe 76

9.1 Es wird keine WAN-Verbindung aufgebaut 76

9.2 DSL-Übertragung langsam 76

9.3 Unerwünschte Verbindungen mit Windows XP 77

9.4 Kabel testen 77

10 Anhang 79

10.1 Leistungs- und Kenndaten 79

10.2 Anschlussbelegung 81
10.2.1 ADSL-Schnittstelle 81
10.2.2 Ethernet WAN-Schnittstelle (LANCOM 1711 VPN) 82
10.2.3 ISDN-S0-Schnittstelle 82
10.2.4 Ethernet-Schnittstellen 10/100Base-T 83
10.2.5 Konfigurationsschnittstelle (Outband) 83

10.3 CE-Konformitätserklärungen 83

11 Index 84

DE

1 Einleitung

Die LANCOM-Modelle LANCOM 821 ADSL/ISDN, LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN sind vollwertige Router und ermöglichen mit der integrierte Firewall einen sicheren Internetzugang für das lokale Netzwerk.

Mit der integrierten oder nachträglich aktivierten VPN-Option arbeiten die Geräte LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN als leistungsfähige Dynamic VPN Gateways für Außenstellen oder mobile Nutzer.

Neben dem DSL- oder ADSL-Anschluss verfügen die Geräte auch über einen ISDN-Anschluss. Die ISDN-Leitung kann als Backup für die DSL-Verbindung genutzt werden, zum Remote Management des Routers, als Basis für die Office-Kommunikation über die LANCAPI und zum Aufbau von Dynamic VPN Verbindungen zu Außenstellen mit dynamischen IP-Adressen.

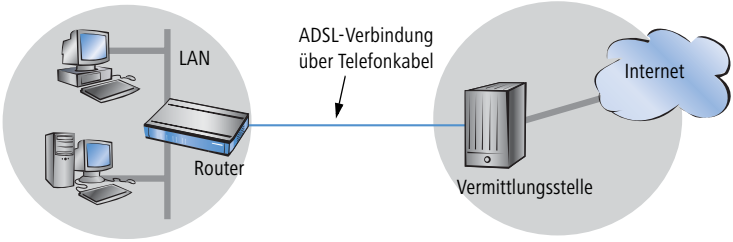
1.1 Wie funktioniert ADSL?

Nur für LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN

Schon Ende der 80er Jahre arbeiteten Wissenschaftler an der Idee, gewöhnliche Telefon-Anschlussleitungen für die Übertragung von Video- und Multimedia-Anwendungen nutzbar zu machen.

Highspeed über herkömmliche Telefonkabel

Dabei verfolgte man den Ansatz, den Telefonanschluss des Teilnehmers nur bis zur nächsten Vermittlungsstelle zu verwenden. Ab der Vermittlungsstelle werden die Daten über Hochgeschwindigkeitsverbindungen zum gewünschten Ziel bzw. ins Zielnetzwerk (etwa das Internet) weitergeleitet. Diese Verkürzung der verwendeten Telefonkabelstrecke auf ein Minimum ermöglicht erheblich größere Übertragungsraten als sie bei kompletter Verwendung des Telefonnetzes möglich sind.



Auf diesem Konzept basieren alle DSL-Technologien, von denen ADSL die weiteste Verbreitung hat. DSL-Verbindungen eignen sich aufgrund ihrer hohen Übertragungsgeschwindigkeit ideal für die Internet-Anbindung.

Ideal für Internet-Surfer

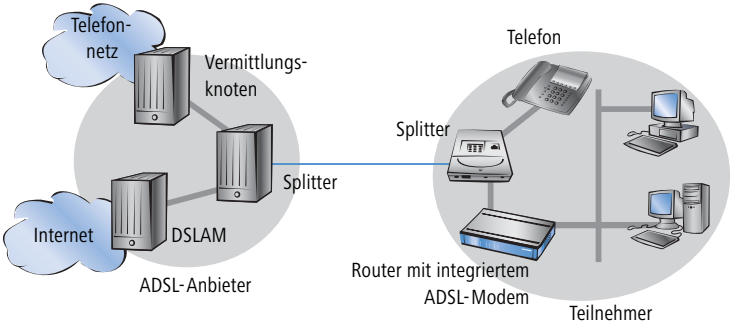
Die DSL-Variante ADSL wurde für Anwendungen entwickelt, bei denen der Teilnehmer große Datenmengen empfängt, selber jedoch nur verhältnismäßig wenig Daten sendet. Typisches Beispiel ist der Zugriff auf das World-Wide-Web (WWW). Nur einige wenige Kommandos (Mausklicks) sind erforderlich, um mitunter sehr große Datenmengen (Grafiken, Texte, Audio, Video) herunter zu laden. Der Benutzer schickt dabei typischerweise nur kleine Datenmengen über die Internetverbindung.

Über eine ADSL-Verbindung kann der Teilnehmer bis zu 8 Mbit/Sekunde empfangen („downstream") und 800 Kbit/Sekunde senden („upstream"). Diese Maximalraten können vom ADSL-Anbieter beliebig reduziert werden. Typische Angebote sind beispielsweise 768 Kbit/Sekunde Download- und 128 Kbit/Sekunde Upload-Geschwindigkeit.

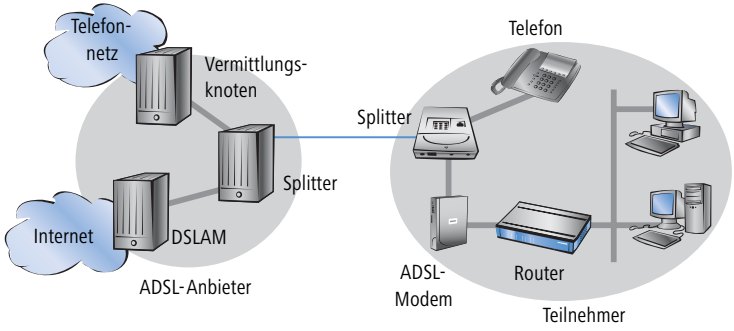
Alle Dienste über ein Kabel – der Splitter macht's möglich

Bei ADSL können parallel zur Datenübertragung auch alle klassischen Telefonie-Anwendungen (Telefon, Fax, Anrufbeantworter, Nebenstellenanlage) ohne Einschränkung weiter genutzt werden. Zu diesem Zweck kommen sogenannte „Splitter" zum Einsatz. Splitter sind Geräte, die auf der Telefonleitung die „Sprachfrequenzen" von den „Datenfrequenzen" trennen und für die Weiterleitung in die jeweiligen Netze sorgen. Sprachsignale werden an das bestehende Telefonnetz übergeben, während die Datensignale über leistungsfähige Netzwerkverbindungen zum Ziel (etwa zum Internetanbieter) geleitet werden.

Auch auf der Teilnehmerseite kommt ein Splitter zum Einsatz und ermöglicht den gleichzeitigen Anschluss von Routern und herkömmlichen Telefonendgeräten.



In manchen Geräte wie auf dem Bild oben ist das ADSL-Modem direkt in den Router integriert (z.B. LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN). Bei der anderen Variante wie beim LANCOM 1711 VPN schließen Sie den Router über ein separates ADSL-Modem an den Splitter an.



Das Modell LANCOM 1711 VPN kann für den Zugang zum Internet auch einen anderen Breitbandanschluss (z.B. ein Kabelmodem) nutzen, der einen 10/100Base-Tx-Ethernetanschluss über PPPoE, PPTP oder einfaches Ethernet anbietet (mit oder ohne DHCP).

Die Modelle LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN können diese Option ebenfalls nutzen, indem der erste LAN-Port als WAN-Interface konfiguriert wird.

DE

ADSL-over-ISDN oder ADSL-over-POTS?

Der Betrieb von ADSL ist sowohl über moderne ISDN- als auch über herkömmliche analoge Telefonanschlüsse (POTS – **P**lain **O**ld **T**elephone **S**ervice) möglich.

Allerdings existieren für die beiden Telefonsysteme unterschiedliche technische Spezifikationen. Aus diesem Grund werden die Geräte mit integriertem ADSL-Modem jeweils in zwei Versionen angeboten: Eine Version für ADSL-over-POTS und eine für ADSL-over-ISDN.

Die Angabe des unterstützten Telefonsystems finden Sie auf der Typenbezeichnung auf der Unterseite des Geräts. Der Gerätename ist auf dem Etikett mit einem Zusatz versehen, der für das unterstützte Telefonsystem steht:

Zusatz	Unterstütztes Telefonsystem
'Annex A'	ADSL-over-POTS
'Annex B'	ADSL-over-ISDN

Ein Gerät vom Typ 'Annex A' kann ausschließlich an ADSL-over-POTS-Anschlüssen betrieben werden. Ein Gerät vom Typ 'Annex B' kann ausschließlich an einem ADSL-over-ISDN-Anschluss betrieben werden. Welche Variante Sie benötigen, erfahren Sie von Ihrem Netzbetreiber. Die nachträgliche Umrüstung eines Gerätes auf das jeweils andere Telefonsystem ist nicht möglich.

Es existieren auch ADSL-over-ISDN-Anschlüsse, die nicht in Kombination mit einem ISDN-Anschluss, sondern mit einem herkömmlichen analogen Telefonanschluss betrieben werden. In Deutschland sind beispielsweise alle von der Deutschen Telekom AG bereitgestellten T-DSL-Anschlüsse als ADSL-over-ISDN-Anschlüsse ausgeführt.

1.2 Welchen Nutzen bietet VPN?

Nur für LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN

Mit einem VPN (**V**irtual **P**rivate **N**etwork) können sichere Datenverkehrsverbindungen über kostengünstige, öffentliche IP-Netze aufgebaut werden, beispielsweise über das Netz der Netze: das Internet.

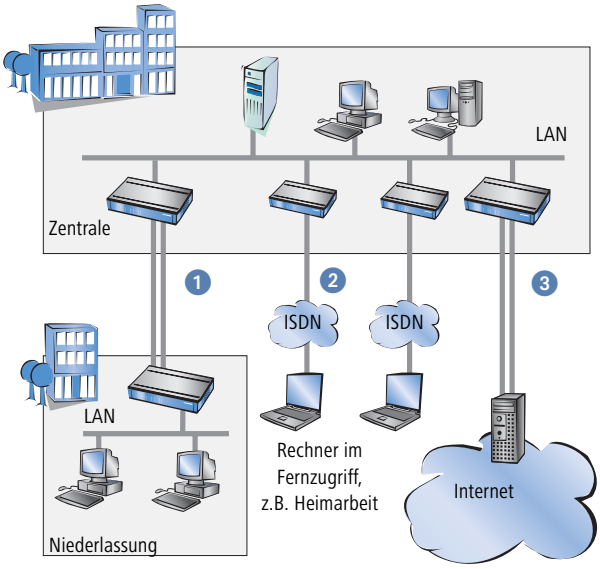
Die Modelle LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN sind ab der LCOS-Version 3.32 standardmäßig mit VPN-Unterstützung für 5 aktive Tunnel ausgestattet. Mit der zusätzlichen LANCOM VPN

Option kann die VPN-Unterstützung auf 25 aktive Tunnel erweitert werden. Die VPN-25 Option aktiviert zusätzlich den beim LANCOM 1711 VPN vorhandenen VPN-Hardware-Beschleuniger.

Was sich zunächst unspektakulär anhört, hat in der Praxis enorme Auswirkungen. Zur Verdeutlichung schauen wir uns zunächst ein typisches Unternehmensnetzwerk ohne VPN-Technik an. Im zweiten Schritt werden wir dann sehen, wie sich dieses Netzwerk durch den Einsatz von VPN optimieren lässt.

Herkömmliche Netzwerkstruktur

Blicken wir zunächst auf eine typische Netzwerkstruktur, die in dieser oder ähnlicher Form in vielen Unternehmen anzutreffen ist:



Das Unternehmensnetz basiert auf einem internen Netzwerk (LAN) in der Zentrale. Dieses LAN ist über folgende Wege mit der Außenwelt verbunden:

1. Eine Niederlassung ist (typischerweise über eine Standleitung) angeschlossen.
2. Rechner wählen sich über ISDN oder Modem ins zentrale Netzwerk ein (Remote Access Service – RAS).

DE

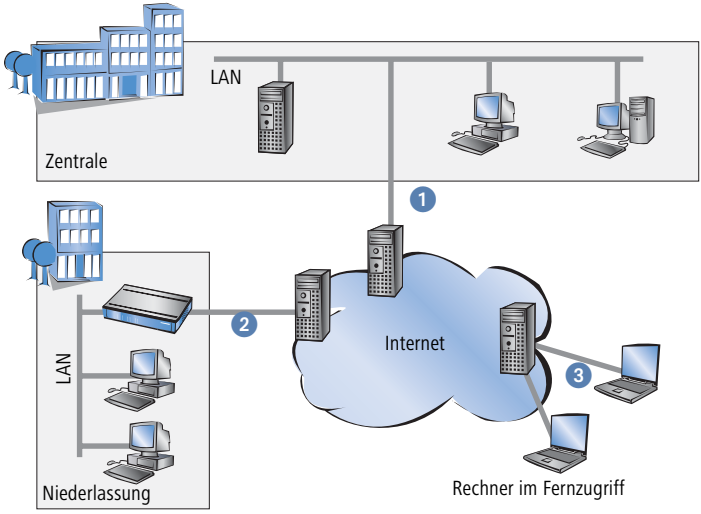
3 Es existiert eine Verbindung ins Internet, um den Benutzern des zentralen LAN den Zugriff auf das Web und die Möglichkeit zum Versand und Empfang von E-Mails zu geben.

Alle Verbindungen zur Außenwelt basieren auf dedizierten Leitungen, d.h. Wähl- oder Standleitungen. Dedizierte Leitungen gelten einerseits als zuverlässig und sicher, andererseits aber auch als teuer. Ihre Kosten sind in aller Regel von der Verbindungsdistanz abhängig. So hat es gerade bei Verbindungen über weite Strecken Sinn, nach preisgünstigeren Alternativen Ausschau zu halten.

In der Zentrale muss für jeden verwendeten Zugangs- und Verbindungsweg (analoge Wählverbindung, ISDN, Standleitungen) entsprechende Hardware betrieben werden. Neben den Investitionskosten für diese Ausrüstung fallen auch kontinuierliche Administrations- und Wartungskosten an.

Vernetzung über Internet

Bei Nutzung des Internets anstelle direkter Verbindungen ergibt sich folgende Struktur:



Alle Teilnehmer sind (fest oder per Einwahl) mit dem Internet verbunden. Es gibt keine teueren dedizierten Leitungen zwischen den Teilnehmern mehr.

1 Nur noch die Internet-Verbindung des LANs der Zentrale ist notwendig. Spezielle Einwahlgeräte oder Router für dedizierte Leitungen zu einzelnen Teilnehmern entfallen.

2. Die Niederlassung ist ebenfalls mit einer eigenen Verbindung ans Internet angeschlossen.
3. Die RAS-Rechner wählen sich über das Internet in das LAN der Zentrale ein.

Das Internet zeichnet sich durch geringe Zugangskosten aus. Insbesondere bei Verbindungen über weite Strecken sind gegenüber herkömmlichen Wähl- oder Standverbindungen deutliche Einsparungen zu erzielen.

Die physikalischen Verbindungen bestehen nicht mehr direkt zwischen zwei Teilnehmern, sondern jeder Teilnehmer hat selber nur einen Zugang ins Internet. Die Zugangstechnologie spielt dabei keine Rolle: Idealerweise kommen Breitbandtechnologien wie DSL (Digital Subscriber Line) zum Einsatz. Aber auch herkömmliche ISDN-Verbindungen können verwendet werden.

Die Technologien der einzelnen Teilnehmer müssen nicht kompatibel zueinander sein, wie das bei herkömmlichen Direktverbindungen erforderlich ist. Über einen einzigen Internet-Zugang können mehrere gleichzeitige logische Verbindungen zu verschiedenen Gegenstellen aufgebaut werden.

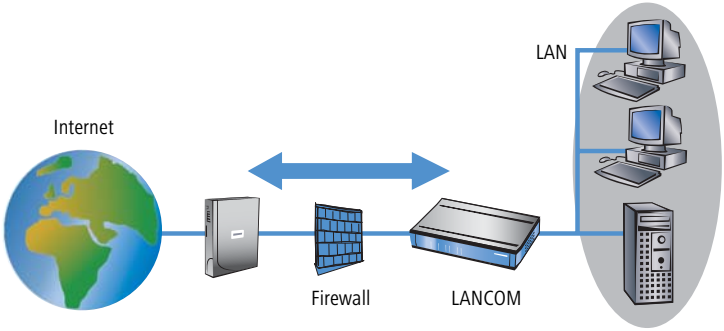
Niedrige Verbindungskosten und hohe Flexibilität machen das Internet (oder jedes andere IP-Netzwerk) zu einem hervorragenden Übertragungsmedium für ein Unternehmensnetzwerk.

1.3 Firewall

Die integrierte Stateful-Inspection Firewall verhindert wirksam ein Eindringen von ungewolltem Datenverkehr in das eigene Netzwerk, indem eingehender Datenverkehr nur als Reaktion auf ausgehenden Datenverkehr zugelassen wird. Die IP-Masquerading-Funktion im Router versteckt beim Zugang ins Internet alle Arbeitsstationen im LAN hinter einer einzigen öffentlichen IP-Adresse. Die tatsächlichen Identitäten (IP-Adressen) der einzelnen Stationen bleiben verborgen. Firewall-Filter im Router erlauben die gezielte Sperrung von IP-Adressen, Protokollen und Ports. Mit MAC-Adressfiltern kann auch der

DE

Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion des Gerätes gezielt kontrolliert werden.



Weitere wichtige Features der Firewall sind

- Intrusion Detection

  Einbruchsversuche in das lokale Netzwerk oder auf die zentrale Firewall werden über das Intrusion-Detection-System (IDS) des LANCOM erkannt, abgewehrt und protokolliert. Dabei kann zwischen Protokollierung im Gerät (Logging), E-Mail-Benachrichtigung, SNMP-Traps oder SYSLOG-Alarmen gewählt werden.

- Denial-of-Service Protecion

  Angriffe aus dem Internet können neben Einbruchsversuchen auch Angriffe mit dem Ziel sein, die Erreichbarkeit und Funktionstüchtigkeit einzelner Dienste zu blockieren. Daher ist der LANCOM mit entsprechenden Schutzmechanismen ausgestattet, die bekannte Hacker-Angriffe erkennen und die Funktionstüchtigkeit der Router garantieren.

- Quality-of-Service / Traffic management

  Unter dem Oberbegriff Quality-of-Service (kurz: QoS) sind die Funktionen des LANCOM zusammengefasst, die sich mit der Sicherstellung von bestimmten Dienstegüten befassen. Das hat den Vorteil, dass die QoS-Funktionen mit den vorhandenen, mächtigen Klassifizierungsmethoden der Firewall (z.B. Einschränkung auf Subnetze, einzelne Arbeitsstationen oder bestimmte Dienste) erfolgen kann.

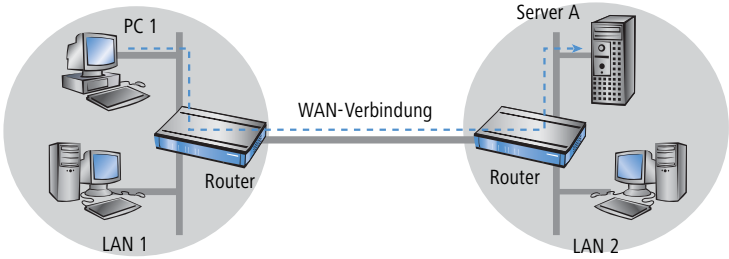
  Mit garantierten Mindestbandbreiten geben Sie Vorfahrt für unternehmenskritische Applikationen, VoIPTK-Anlagen oder bestimmte Benutzergruppen.

Details zur Funktion des Stateful-Inspection Firewall Ihres LANCOM entnehmen Sie dem Referenzhandbuch.

1.4 Was macht ein Router?

Die folgenden Abschnitte beschreiben allgemein die Funktionalität von Routern. Welche Funktionen von Ihrem Gerät unterstützt werden, können Sie der Tabelle 'Was kann Ihr LANCOM?' →Seite 19 entnehmen.

Router verbinden voneinander entfernte LANs und Einzel-PCs miteinander zu einem Wide Area Network (WAN). Jeder Rechner in diesem WAN kann – sofern er dazu berechtigt ist – auf die Rechner und Dienste im gesamten WAN zugreifen (so wie in der Abbildung 'PC 1' auf 'Server A' im entfernten LAN zugreift).



Der Anschluss eines LAN an das Internet unterscheidet sich technisch nicht von der Kopplung zweier LANs. Der einzige Unterschied besteht darin, dass hinter dem Router des Internetanbieters nicht nur einige wenige Rechner stecken, sondern das Netz der Netze.

1.4.1 Brückenkopf zum WAN

Jeder Router verfügt über mindestens zwei Anschlüsse:

- Mindestens einen für das LAN
- Mindestens einen für WAN-Verbindungen

Einige Modelle verfügen neben dem LAN-Anschluss (10/100-Mbit-Ethernet) auch über einen integrierten Switch. Für die Anbindung an das WAN nutzen die Router einen ISDN-, DSL- oder ADSL-Anschluss. Zusätzlich enthalten

manche Geräte eine Funknetzwerkkarte und können damit auch Stationen in WLANs (Wireless LANs) in das Routing mit einbeziehen.

Die Aufgabe des Routers besteht darin, Daten aus dem eigenen LAN über eine geeignete WAN-Verbindung in das Zielnetzwerk zu übermitteln. Ebenso werden Daten aus dem WAN an den gewünschten Empfänger im LAN weitergeleitet.

1.4.2 Einsatzgebiete für Router

Router werden überwiegend für folgende Anwendungen eingesetzt:

- Internet-Zugang für ein LAN (z.B. über DSL oder ISDN)

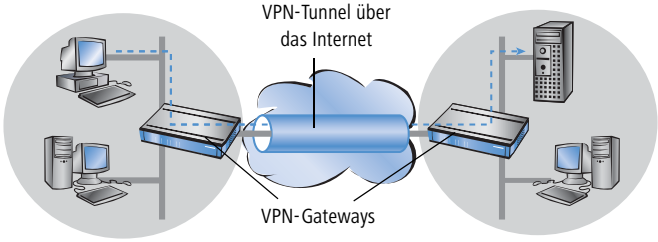
  Das Internet besteht aus unzähligen großen und kleinen Netzwerken, die über Router zum weltgrößten WAN verbunden sind. Ihr Router verbindet alle Arbeitsplatzrechner ihres LAN mit dem globalen Internet. Sicherheitsfunktionen wie IP-Masquerading schirmen Ihr LAN gegen unbefugten Zugriff von außen ab.

- LAN-LAN-Kopplung (über VPN oder ISDN)

  Eine LAN-LAN-Kopplung verbindet zwei LANs zu einem WAN, bei Bedarf sogar über Kontinente hinweg. Typisches Beispiel: Eine Niederlassung soll an das LAN der Zentrale gekoppelt werden. Grundsätzlich können Sie LANs auf zwei Arten koppeln:

  Nicht mit allen LANCOM-Geräten möglich.

  ▷ Highspeed-Kopplung über VPN
  Mit der VPN-Technologie (Virtual Private Network) sind die schnellsten und günstigsten LAN-LAN-Kopplungen möglich, da VPN das Internet als Kommunikationsbasis verwendet. Dabei kommt der schnelle xDSL-Anschluss des Routers zum Einsatz. Voraussetzung: auf beiden Seiten der Netzwerkkopplung wird ein VPN-Gateway mit Zugang zum Internet benötigt.



  ▷ Herkömmlich über ISDN
  Ohne VPN kann eine LAN-LAN-Kopplung alternativ über ISDN aufgebaut werden. In diesem Fall sorgt ein intelligentes Line-Management

im Zusammenspiel mit ausgefeilten Filtermechanismen für geringe Verbindungskosten.

- Fernzugriff auf das Firmennetz (über VPN oder ISDN)

  Die Arbeit vieler Mitarbeiter in modernen Organisationen wird immer unabhängiger von bestimmten Orten – wichtig ist vor allem der ständige Zugriff auf gemeinsame, frei verfügbare Informationen.

  Remote-Access-Service (RAS) heißt hier das Zauberwort. Heimarbeitsplätze oder Außendienstmitarbeiter wählen sich über VPN oder ISDN ins zentrale Netzwerk ein. Beim Remote-Access über ISDN schützt der Router das firmeneigene Netzwerk: Die Rückruffunktion erlaubt nur bekannten und registrierten Personen Zugang.

1.5 Was kann Ihr LANCOM?

Die folgende Tabelle zeigt Ihnen die Eigenschaften und Funktionen Ihres Gerätes im unmittelbaren Modellvergleich.

	LANCOM 821 ADSL	LANCOM 1621 ADSL	LANCOM 1711 DSL
Anwendungen			
Internet-Zugang	✓	✓	✓
LAN-LAN-Kopplung über VPN		✓	✓
LAN-LAN-Kopplung über ISDN	✓	✓	✓
RAS-Server (über VPN)		✓	✓
RAS-Server (über ISDN)	✓	✓	✓
IP-Router	✓	✓	✓
IPX-Router (über ISDN), z.B. zur Kopplung von Novell-Netzwerken oder zur Einwahl in Novell-Netzwerke	✓	✓	✓
NetBIOS-Proxy zur Kopplung von Microsoft-Peer-to-Peer-Netzwerken über ISDN	✓	✓	✓
DHCP- und DNS-Server (für LAN und WAN)	✓	✓	✓

	LANCOM 821 ADSL	LANCOM 1621 ADSL	LANCOM 1711 DSL
N:N-Mapping zur Kopplung von bestehenden Netzwerken mit gleichen IP-Adresskreisen		✓	✓
LANCAPI-Server für den Einsatz von Office-Anwendungen wie Fax oder Anrufbeantworter über die ISDN-Schnittstelle.	✓	✓	✓
WAN-Anschlüsse			
Anschluss für DSL- oder Kabelmodem	✓	✓	✓
integriertes ADSL-Modem	✓	✓	
ISDN-S_0-Anschluss in Punkt-zu-Mehrpunkt-Konfiguration (Mehrgeräteanschluss) oder in Punkt-zu-Punkt-Konfiguration (Anlagenanschluss) mit automatischer D-Kanal-Protokoll-Erkennung. Unterstützt statische und dynamische Kanalbündelung per MLPPP und BACP sowie Stac-Datenkompression (Hi/fn). Auch zum Aufbau von Dynamic VPN-Verbindungen zu Gegenstellen mit dynamischen IP-Adressen.	✓	✓	✓
LAN-Anschluss			
Integrierter 4 Port Auto-Mode-Switch (10/100 Mbit) mit „Private Mode" zur Abschirmung der Ports untereinander	✓	✓	
4 individuelle Fast Ethernet LAN Ports, einzeln schaltbar, z.B. als LAN-Switch oder separate DMZ-Ports, Auto-Crossover.			✓
Sicherheitsfunktionen			
IPSec-Verschlüsselung über externe Software (VPN-Client)	✓	✓	✓
IPSec-Verschlüsselung über interne Software		✓	✓
IPSec-Verschlüsselung über Hardware (optional, Aktivierung über VPN-25-Option)			✓
IP-Masquerading (NAT, PAT) zum Verstecken aller Arbeitsstationen im LAN hinter einer einheitlichen öffentlichen IP-Adresse.	✓	✓	✓
Stateful-Inspection Firewall	✓	✓	✓
Firewall-Filter zur gezielten Sperrung von IP-Adressen, Protokollen und Ports.	✓	✓	✓
MAC-Adressfilter kontrolliert u.a. den Zugriff von Arbeitsstationen im LAN auf die IP-Routing-Funktion.	✓	✓	✓
Konfigurationsschutz zur Abwehr von „Brute-Force-Angriffen".	✓	✓	✓
Konfiguration			

	LANCOM 821 ADSL	LANCOM 1621 ADSL	LANCOM 1711 DSL
Konfiguration mit LANconfig oder mit Webbrowser, zusätzlich Terminal-modus für Telnet oder andere Terminalprogramme, SNMP-Schnittstelle und TFTP-Serverfunktion.	✓	✓	✓
Fernkonfiguration über ISDN (mit ISDN-PPP-Verbindungen z. B. über das DFÜ-Netzwerk von Windows).	✓	✓	✓
Serielle Konfigurations-Schnittstelle	✓	✓	✓
Rückruf-Funktion mit PPP-Authentifizierung-Mechanismen zur Beschränkung auf festgelegte ISDN-Rufnummern.	✓	✓	✓
FirmSafe zum Einspielen neuer Firmwareversionen ohne Risiko.	✓	✓	✓
Optionale Software-Erweiterungen			
ISDN-Festverbindungsoption	✓	✓	✓
LANCOM VPN Option mit 25 aktiven Tunneln zur Absicherung von Netzwerkkopplungen		✓	✓

DE

2 Installation

Dieses Kapitel hilft Ihnen, möglichst schnell Hard- und Software zu installieren. Zunächst überprüfen Sie Lieferumfang und Systemvoraussetzungen. Sind alle Voraussetzungen erfüllt, gelingen Anschluss und Inbetriebnahme schnell und ohne Mühe.

2.1 Lieferumfang

Bitte prüfen Sie den Inhalt der Verpackung auf Vollständigkeit, bevor Sie mit der Installation beginnen. Neben dem eigentlichen Gerät sollte der Karton folgendes Zubehör für Sie bereithalten:

	LANCOM 821 ADSL/ISDN	LANCOM 1621 ADSL/ISDN	LANCOM 1711 DSL
Netzteil	✓	✓	✓
LAN-Anschlusskabel (grüne Stecker)	✓	✓	✓
WAN-Anschlusskabel (dunkelblaue Stecker)			✓
ADSL-Anschlusskabel (transparente Stecker)	✓	✓	
ISDN-Anschlusskabel (hellblaue Stecker)	✓	✓	✓
Anschlusskabel für die Konfigurationsschnittstelle	✓	✓	✓
LANCOM-CD	✓	✓	✓
Gedruckte Dokumentation	✓	✓	✓

Falls etwas fehlen sollte, wenden Sie sich bitte umgehend an Ihren Händler oder an die Kontaktadresse, die auf dem Lieferschein zu Ihrem Gerät angegeben ist.

2.2 Systemvoraussetzungen

Rechner, die mit einem LANCOM in Verbindung treten möchten, müssen mindestens die folgenden Voraussetzungen erfüllen:

- Betriebssystem mit TCP/IP-Unterstützung, z. B. Windows XP, Windows Millennium Edition (Me), Windows 2000, Windows 98, Windows 95, Windows NT, Linux, BSD Unix, Apple Mac OS, OS/2, BeOS.
- Zugang zum LAN über das TCP/IP-Protokoll.

Die LANtools und die Funktionen der LANCAPI benötigen zudem ein Windows-Betriebssystem. Für den Zugriff auf WEBconfig ist ein Web-Browser erforderlich.

2.3 LANCOM stellt sich vor

In diesem Abschnitt stellen wir Ihnen Ihr Gerät vor. Sie erhalten einen Überblick über alle Statusanzeigen, Anschlüsse und Schalter.

Für die Installation des Gerätes ist dieser Abschnitt hilfreich aber nicht unbedingt erforderlich. Sie können diesen Abschnitt nach Belieben auch erst einmal überschlagen und direkt mit dem Abschnitt 'Installation der Hardware' →Seite 30 fortfahren.

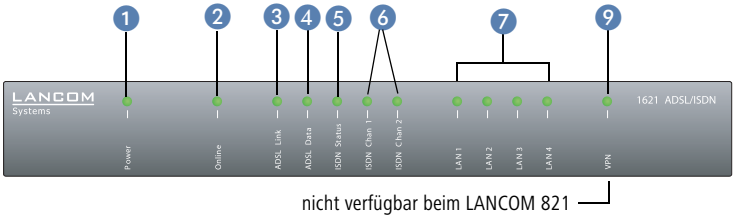
2.3.1 Statusanzeigen

Die verschiedenen LANCOM-Modelle verfügen je nach Funktionsumfang über eine unterschiedliche Anzahl von Statusanzeigen auf der Vorderseite.

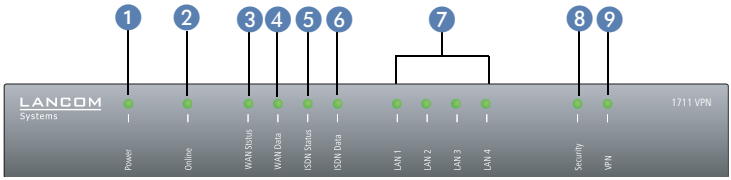
Vorderseite

Die verschiedenen LANCOM-Modelle verfügen je nach Funktionsumfang über eine unterschiedliche Anzahl von Statusanzeigen auf der Vorderseite:

LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN



LANCOM 1711 VPN



Oberseite

Die beiden LEDs auf der Oberseite ermöglichen ein bequemes Ablesen der wichtigsten Statusanzeigen auch bei vertikaler Befestigung des Gerätes.

Bedeutung der LEDs

In den folgenden Abschnitten verwenden wir verschiedene Begriffe, um das Verhalten der LEDs zu beschreiben:

- **Blinken** bedeutet, dass die LED in gleichmäßigen Abständen in der jeweils angegebenden Farbe ein- bzw. ausgeschaltet wird.
- **Blitzen** bedeutet, dass die LED in der jeweiligen Farbe sehr kurz aufleuchtet und dann deutlich länger (etwa 10x so lange) ausgeschaltet bleibt.
- **Invers Blitzen** bedeutet das Gegenteil. Hier leuchtet die LED in der jeweiligen Farbe dauerhaft und wird nur sehr kurz unterbrochen.
- **Flackern** bedeutet, dass die LED in unregelmäßigen Abständen ein- und ausgeschaltet wird.

Power 1

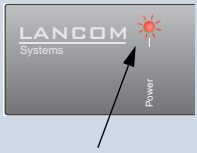
Diese LED gibt Auskunft über die Betriebsbereitschaft des Geräts. Nach dem Einschalten blinkt sie für die Dauer des Selbsttests grün. Danach wird entwe-

der ein festgestellter Fehler als roter Blinkcode ausgegeben, oder aber das Gerät geht in Betrieb, und die LED leuchtet konstant grün.

aus		Gerät abgeschaltet
grün	blinkend	Selbsttest nach dem Einschalten
grün	dauerhaft an	Gerät betriebsbereit
rot/grün	abwechselnd blinkend	Gerät unsicher: Kein Konfigurationskennwort gesetzt
rot	blinkend	Zeit- oder Gebührenlimit erreicht

Die Power-LED blinkt abwechselnd rot/grün, solange noch kein Konfigurationskennwort gesetzt wurde. Ohne Konfigurationskennwort sind die Konfigurationsdaten des LANCOM ungeschützt. Im Normalfall setzen Sie ein Konfigurationskennwort während der Grundkonfiguration (Anleitung im folgenden Kapitel). Informationen zur nachträglichen Vergabe eines Konfigurationskennworts finden Sie im Abschnitt 'Der Sicherheits-Assistent' auf Seite 70.

Blinkende Power-LED und keine Verbindung möglich?



Signal für ein erreichtes Zeit- oder Gebührenlimit

Blinkt die Power-LED rot, und können keine WAN-Verbindungen mehr aufgebaut werden, so ist das kein Grund zur Besorgnis. Vielmehr wurde ein vorher eingestelltes Zeit- oder Gebührenlimit erreicht. Es gibt drei Möglichkeiten die Sperre zu lösen:

- Gebührenschutz zurücksetzen.
- Das erreichte Limit erhöhen.
- Die erreichte Sperre ganz deaktivieren (Limit auf '0' setzen).

Unter LANmonitor wird Ihnen das Erreichen eines Zeit- oder Gebührenlimits angezeigt. Zum Reset des Gebührenschutzes wählen Sie im Kontextmenü (rechter Mausklick) **Zeit- und Gebühren-Limits zurücksetzen**. Die Gebühreneinstellungen legen Sie in LANconfig unter **Management** ▶ **Kosten** fest (Sie können nur dann auf diese Einstellungen zugreifen, wenn unter **Ansicht** ▶ **Option…** die 'Vollständige Darstellung der Konfiguration' aktiviert ist).

Mit WEBconfig finden Sie den Gebührenschutz-Reset und alle Parameter unter **Experten-Konfiguration** ▶ **Setup** ▶ **Gebühren-Modul**.

Online 2

Das Online-LED zeigt allgemein den Status aller WAN-Schnittstellen an:

aus		keine aktive Verbindung
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau einer weiteren Verbindung
grün	dauerhaft an	mindestens eine Verbindung aufgebaut
rot	dauerhaft an	Fehler beim Aufbau der letzten Verbindung

ADSL Link (nur LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN) 3

Verbindungszustand am ADSL-Anschluss:

aus		nicht angeschlossen
grün	blinkend	Initialisierung (Kontaktaufnahme mit Verbindungsstelle)
grün		Synchronisation erfolgreich
rot	flackernd	Fehler (CRC-Fehler, Framing-Fehler etc.)
rot		Synchronisation fehlgeschlagen

WAN Status (nur LANCOM 1711 VPN) 3

Verbindungszustand am WAN-Anschluss:L

aus		keine Verbindung
grün	blinkend	Aufbau der Verbindung
grün	blitzend	Protokollverhandlung
grün	dauerhaft an	Verbindung aufgebaut

ADSL Data (nur LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN) 4

Anzeige von Datenverkehr am ADSL-Anschluss:

aus		keine Verbindung
grün	blitzend	Aufbau der ersten Verbindung
grün	invers blitzend	Aufbau einer weiteren Verbindung
grün	dauerhaft an	mindestens eine Verbindung aufgebaut
grün	invers flackernd	Datenverkehr (Versand oder Empfang)

WAN Data (nur LANCOM 1711 VPN) 4

Anzeige von Datenverkehr am WAN-Anschluss:

aus		keine Verbindung
grün	dauerhaft an	Verbindung aufgebaut
grün	flackernd	Datenverkehr (Versand oder Empfang)
rot	flackernd	Kollision von Datenpaketen

ISDN Status 5

Verbindungsstatus am ISDN-S_0-Anschluss:

aus		nicht angeschlossen oder keine S_0-Spannung (keine Fehlermeldung)
grün	blinkend	Initialisierung D-Kanal (Kontaktaufnahme mit Verbindungsstelle)
grün	dauerhaft an	D-Kanal betriebsbereit
rot	flackernd	Fehler auf dem D-Kanal
rot	dauerhaft an	D-Kanal-Aktivierung fehlgeschlagen

Wenn die ISDN-Status-LED automatisch erlischt, so ist dies kein Zeichen für einen Fehler am S_0-Bus. Vielmehr schalten zahlreiche ISDN-Anschlüsse und Telefonanlagen den S_0-Bus nach einer bestimmten inaktiven Zeit in einen Stromsparmodus. Bei Bedarf wird der S_0-Bus automatisch reaktiviert und die ISDN-Status-LED leuchtet grün.

ISDN Chan 1
ISDN Chan 2
(nur LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN) 6

ISDN Data (nur LANCOM 1711 VPN) 6

Separate Statusanzeige für beide ISDN-B-Kanäle:

aus		keine Verbindung aufgebaut
grün	blinkend	Anwahl läuft
grün	blitzend	Aufbau der ersten Verbindung
grün	dauerhaft an	Verbindung über B-Kanal aufgebaut
grün	invers flackernd	Datenverkehr (Versand oder Empfang)

DE

LAN 1
LAN 2
LAN 3
LAN 4 7

Zustand der vier LAN-Anschlüsse im integrierten Switch:

aus		kein Netzwerkgerät angeschlossen
grün	dauerhaft an	Verbindung zu Netzwerkgerät betriebsbereit, kein Datenverkehr
grün	flackernd	Datenverkehr
rot	flackernd	Kollision von Datenpaketen

Security (nur LANCOM 1711 VPN) 8

Status der Firewall. Zeigt den Zustand der Sicherheitseinstellungen und abgewehrte Angriffe auf das geschützte Netzwerk an.

grün	dauerhaft an	Sicherheitseinstellungen OK. Paketfilter-Regeln sind eingerichtet.
rot/grün	blinkend	Unsichere Konfiguration
rot	flackernd	Sicherheitsalarm: Datenpaket gefiltert durch Firewall-Regeln

VPN (nur LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN) 9

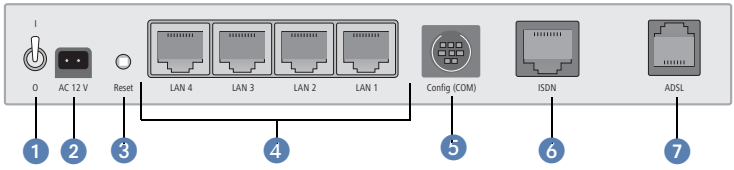
Status einer VPN-Verbindung. Nur bei installierter LANCOM VPN Option aktiv.

aus		kein VPN-Tunnel aufgebaut
grün	blinkend	Verbindungsaufbau
grün	blitzend	Erste Verbindung
grün	invers blitzend	Weitere Verbindungen
grün	dauerhaft an	VPN-Tunnel ist aufgebaut

2.3.2 Die Anschlüsse des Geräts

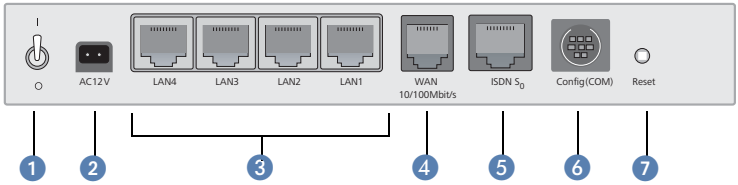
Auf der Rückseite befinden sich die Anschlüsse und Schalter des Routers:

LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN



1. Netzschalter
2. Anschluss für das mitgelieferte Netzteil
3. Reset-Schalter
4. Switch mit vier 10/100Base-Tx-Anschlüssen.
5. Serielle Konfigurationsschnittstelle
6. ISDN/S_0-Anschluss
7. ADSL-Anschluss

LANCOM 1711 VPN



1. Netzschalter
2. Anschluss für das mitgelieferte Netzteil
3. Switch mit vier 10/100Base-Tx-Anschlüssen
4. WAN-Anschluss
5. ISDN/S_0-Anschluss
6. Serielle Konfigurationsschnittstelle
7. Reset-Schalter

   Der Reset-Schalter hat zwei verschiedene Funktionen, die durch unterschiedlich lange Betätigungszeiten des Tasters ausgelöst werden:

   - **Neustart des Geräts** (weicher Reset) – der Schalter wird kürzer als 5 Sekunden gedrückt. Das Gerät startet neu.
   - **Zurücksetzen der Konfiguration** (harter Reset) – der Schalter wird länger als 5 Sekunden gedrückt. Alle LEDs am Gerät leuchten dauerhaft auf. Sobald der Reset-Schalter freigegeben wird startet das Gerät mit Werkseinstellungen neu.

DE

2.4 Installation der Hardware

Die Installation des LANCOM erfolgt in folgenden Schritten:

① **LAN** – schließen Sie Ihren LANCOM zunächst ans LAN oder einen einzelnen PC an. Stecken Sie das mitgelieferte Netzwerkkabel (grüne Stecker) einerseits in einen LAN-Anschluss des Geräts 4 (LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN) bzw. 3 (LANCOM 1711 VPN) und andererseits in eine freie Netzwerkanschlussdose Ihres lokalen Netzes, eine freie Buchse eines Switches/Hubs oder den Netzwerkeingang eines einzelnen PC.

Die LAN-Anschlüsse erkennen sowohl die Übertragungsrate (10/100 Mbit) als auch den Typ (Node/Hub) angeschlossener Netzwerkgeräte automatisch (Autosensing). Der parallele Anschluss von Geräten unterschiedlicher Geschwindigkeit und Typen ist möglich.

In einem Netzwerksegment sollten sich niemals mehrere unkonfigurierte LANCOM gleichzeitig befinden. Alle unkonfigurierten LANCOM melden sich unter derselben IP-Adresse (mit den Endziffern '254'), es kommt daher zu Adresskonflikten. Zur Vermeidung von Problemen sollten mehrere LANCOM immer nacheinander konfiguriert und jeweils sofort mit einer eindeutigen IP-Adresse (die nicht auf '254' endet) versehen werden.

nur 821/1621

② **ADSL** – verbinden Sie die ADSL-Schnittstelle 7 über das mitgelieferte ADSL-Anschlusskabel (transparente Stecker) mit dem Splitter.

nur 1711

③ **DSL** – verbinden Sie die WAN-Schnittstelle 4 über das mitgelieferte DSL-Anschlusskabel (dunkelblaue Stecker) mit dem ADSL-Modem.

④ **ISDN** – für den Anschluss des LANCOM an das ISDN stecken Sie das eine Ende des mitgelieferten ISDN-Anschlusskabels (hellblaue Stecker) in die ISDN/S_0-Schnittstelle 6 (LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN) bzw. 5 (LANCOM 1711 VPN) des Routers und das andere Ende in einen ISDN/S_0-Anlagenanschluss oder -Mehrgeräteanschluss.

⑤ **Konfigurations-Schnittstelle** – optional können Sie den Router direkt an die serielle Schnittstelle (RS-232, V.24) eines PC anschließen. Verwenden Sie dazu das mitgelieferte Anschlusskabel. Verbinden Sie die Konfigurations-Schnittstelle des LANCOM 5 (LANCOM 821 ADSL/ISDN und

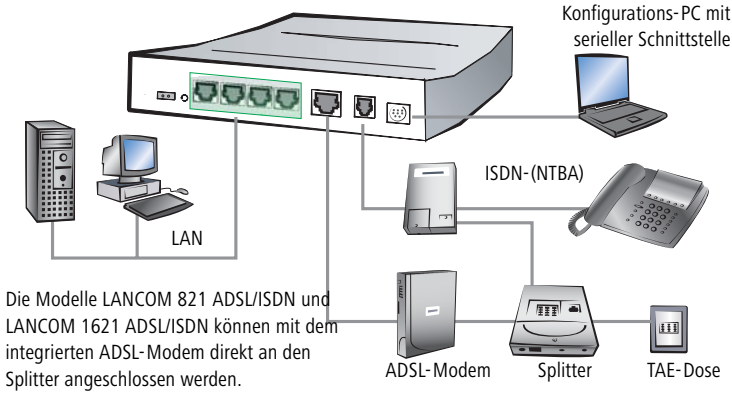
LANCOM 1621 ADSL/ISDN) bzw. 6 (LANCOM 1711 VPN) mit einer freien seriellen Schnittstelle des PC.

⑥ **Mit Spannung versorgen** – versorgen Sie das Gerät an Buchse 2 über das mitgelieferte Netzteil mit Spannung.

Verwenden Sie ausschließlich das mitgelieferte Netzteil! Die Verwendung eines ungeeigneten Netzteils kann zu Personen- oder Sachschäden führen.

⑦ **Betriebsbereit?** – Nach einem kurzen Selbsttest des Geräts leuchtet die Power-LED permanent. Grün leuchtende LAN-LEDs zeigen an, an welchen LAN-Anschlüssen funktionierende Verbindungen hergestellt sind.

Beispielzeichnung für das Modell LANCOM 1711 VPN


Konfigurations-PC mit serieller Schnittstelle
ISDN-(NTBA)
LAN
Die Modelle LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN können mit dem integrierten ADSL-Modem direkt an den Splitter angeschlossen werden.
ADSL-Modem
Splitter
TAE-Dose

Die Geräte mit integriertem ADSL-Modem können im Betrieb recht warm werden. Bei diesen Modellen ist insbesondere der Umgebungstemperaturbereich von max. 35°C zu beachten. Für eine ausreichende Belüftung ist zu sorgen. Geräte nicht stapeln und keiner direkten Sonneneinstrahlung aussetzen!

2.5 Installation der Software

Der folgende Abschnitt beschreibt die Installation der mitgelieferten Systemsoftware LANtools, die unter Windows läuft.

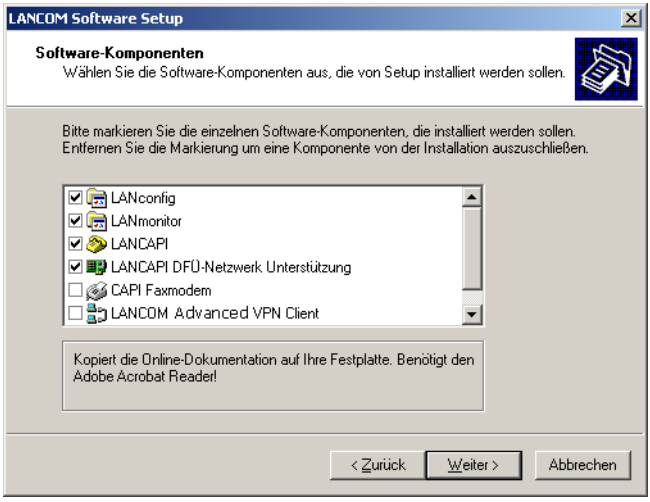
Sollten Sie Ihren LANCOM ausschließlich mit PCs verwenden, die unter anderen Betriebssystemen als Windows laufen, können Sie diesen Abschnitt überspringen.

2.5.1 LANCOM-Setup starten

Legen Sie die LANCOM-CD in Ihr Laufwerk ein. Daraufhin startet das LANCOM-Setup-Programm automatisch.

Sollte das Setup nicht automatisch starten, so rufen Sie die Datei AUTORUN.EXE aus dem Hauptverzeichnis der LANCOM-CD auf.

Klicken Sie im Setup auf **LANCOM Software installieren**. Es erscheint folgendes Auswahlmenü auf dem Bildschirm:


LANCOM Software Setup
Software-Komponenten
Wählen Sie die Software-Komponenten aus, die von Setup installiert werden sollen.
Bitte markieren Sie die einzelnen Software-Komponenten, die installiert werden sollen.
Entfernen Sie die Markierung um eine Komponente von der Installation auszuschließen.
LANconfig
LANmonitor
LANCAPI
LANCAPI DFÜ-Netzwerk Unterstützung
CAPI Faxmodem
LANCOM Advanced VPN Client
Kopiert die Online-Dokumentation auf Ihre Festplatte. Benötigt den Adobe Acrobat Reader!
< Zurück
Weiter >
Abbrechen

2.5.2 Welche Software installieren?

- **LANconfig** ist das Windows-Konfigurationsprogramm für alle LANCOM-Router und Wireless LAN Access Points. Alternativ (oder ergänzend) kann über einen Web-Browser WEBconfig verwendet werden.
- Mit **LANmonitor** überwachen Sie auf einem Windows-Rechner alle LANCOM-Router und Wireless LAN Access Points.

- Die **LANCAPI** ist eine spezielle Form der CAPI-2.0-Schnittstelle, über die alle Arbeitsstationen im LAN Zugriff auf Bürokommunikations-Funktionen wie Fax und EuroFileTransfer erhalten. Mit der **LANCAPI DFÜ Netzwerkunterstützung** können einzelne Rechner über die LANCAPI Einwahlverbindungen zu einem Internetprovider herstellen. Das **CAPI Faxmodem** stellt Ihnen einen Faxtreiber der Klasse 1 zur Verfügung.
- Der **LANCOM VPN Client** ermöglicht den Aufbau von VPN-Verbindungen von einem entfernten Rechner über das Internet zu einem Router mit LANCOM VPN Option.
- Mit **LANCOM Online Dokumentation** kopieren Sie die Dokumentationsdateien auf Ihren PC.

Wählen Sie die gewünschten Software-Optionen aus und bestätigen Sie mit **Weiter**. Die Software wird automatisch installiert.

DE

3 Grundkonfiguration

Die Grundkonfiguration erfolgt mit Hilfe eines komfortablen Setup-Assistenten, der Sie Schritt für Schritt durch die Konfiguration führt und dabei die notwendigen Informationen abfragt.

Dieses Kapitel zeigt Ihnen zunächst, welche Angaben für die Grundkonfiguration erforderlich sind. Mit Hilfe dieses ersten Abschnitts stellen Sie sich schon vor Aufruf des Assistenten alle notwendigen Daten zusammen.

Anschließend erfolgt die Eingabe der Daten im Setup-Assistenten. Aufruf und Ablauf werden Schritt für Schritt beschrieben – in jeweils einem eigenen Abschnitt für LANconfig und WEBconfig. Dank der vorherigen Zusammenstellung aller notwendigen Angaben gelingt die Grundkonfiguration jetzt schnell und ohne Mühe.

Zum Abschluss dieses Kapitels zeigen wir Ihnen, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind, damit der Zugriff auf den Router einwandfrei funktioniert ('TCP/IP-Einstellungen an den Arbeitsplatz-PCs' auf Seite 44).

3.1 Welche Angaben sind notwendig?

Der Grundkonfigurations-Assistent nimmt nacheinander die TCP/IP-Grundeinstellung des Routers vor, schützt des Gerät mit einem Konfigurationskennwort und richtet auf Wunsch auch den ISDN-Anschluss ein. Die folgenden Beschreibungen der vom Assistenten geforderten Angaben gliedert sich in die folgenden Konfigurationsabschnitte:

- TCP/IP-Einstellungen
- Schutz der Konfiguration
- Angaben zum DSL-Anschluss
- Angaben zum ISDN-Anschluss
- Einstellung des Gebührenschutzes

3.1.1 TCP/IP-Einstellungen

Die TCP/IP-Konfiguration kann auf zweierlei Art erfolgen: Entweder vollautomatisch oder manuell. Bei der vollautomatischen TCP/IP-Konfiguration ist keine Benutzereingabe erforderlich. Alle Parameter werden selbstständig vom Setup-Assistenten gesetzt. Bei der manuellen TCP/IP-Konfiguration fragt der Assistent die üblichen TCP/IP-Parameter ab: IP-Adresse, Netzmaske etc. (dazu später mehr).

Die vollautomatische TCP/IP-Konfiguration ist nur in bestimmten Netzwerkumgebungen möglich. Deshalb analysiert der Setup-Assistent das angeschlossene LAN daraufhin, ob die vollautomatische Konfiguration möglich ist oder nicht.

Neues LAN – vollautomatische Konfiguration möglich

Sind alle angeschlossenen Netzwerkgeräte noch unkonfiguriert, dann bietet der Setup-Assistent die vollautomatische TCP/IP-Konfiguration an. Dazu kommt es normalerweise in folgenden Situationen:

- Nur ein Einzelplatz-PC wird an den Router angeschlossen
- Neuaufbau eines Netzwerks

Wenn Sie den LANCOM in ein bestehendes TCP/IP-LAN integrieren, wird die vollautomatische TCP/IP-Konfiguration nicht angeboten. In diesem Fall können Sie mit dem Abschnitt 'Notwendige Angaben für die manuelle TCP/IP-Konfiguration' auf Seite 36 fortfahren.

Das Ergebnis der vollautomatischen TCP/IP-Konfiguration: Der Router erhält die IP-Adresse '172.23.56.1' (Netzmaske '255.255.255.0'). Außerdem wird der integrierte DHCP-Server aktiviert, so dass der LANCOM den Geräten im LAN automatisch IP-Adressen zuweist.

Trotzdem manuell konfigurieren?

Die vollautomatische TCP/IP-Konfiguration ist optional. Sie können stattdessen auch die manuelle Konfiguration wählen. Treffen Sie diese Wahl nach folgenden Überlegungen:

- Wählen Sie die automatische Konfiguration wenn Sie mit Netzwerken und IP-Adressen **nicht** vertraut sind.
- Wählen Sie die manuelle TCP/IP-Konfiguration, wenn Sie mit Netzwerken und IP-Adressen vertraut sind und eine der folgenden Annahmen zutrifft:
  - Sie haben bisher in Ihrem Netzwerk noch keine IP-Adressen verwendet, möchten das ab jetzt aber gerne tun. Sie möchten die IP-Adresse für den Router selbst festlegen und geben ihm eine beliebige Adresse aus einem der für private Zwecke reservierten Adressbereiche, z.B. '10.0.0.1' mit der Netzmaske '255.255.255.0'. Damit legen Sie auch gleichzeitig den Adressbereich fest, den der DHCP-Server anschließend für die anderen Geräte im Netz verwendet (sofern der DHCP-Server aktiviert wird).
  - Sie haben auch bisher schon IP-Adressen auf den Rechnern im LAN verwendet.

Notwendige Angaben für die manuelle TCP/IP-Konfiguration

Bei der manuellen TCP/IP-Konfiguration fragt Sie der Setup-Assistent nach folgenden Daten:

- **IP-Adresse und Netzwerkmaske für den LANCOM**
  Teilen Sie dem LANCOM eine freie IP-Adresse aus dem Adressbereich Ihres LAN zu, und geben Sie die Netzwerkmaske an.
- **DHCP-Server einschalten?**
  Wenn Sie die IP-Adressen in Ihrem LAN über einen anderen DHCP-Server zuweisen, so schalten Sie die DHCP-Server-Funktion im LANCOM aus.

3.1.2 Konfigurationsschutz

Mit dem Kennwort schützen Sie den Konfigurationszugang zum LANCOM und verhindern so, dass Unbefugte diese modifizieren. Die Konfiguration des Routers enthält zahlreiche sensible Daten, wie beispielsweise die Daten für den Internet-Zugang, und sollte auf jeden Fall durch ein Kennwort geschützt sein.

Der Setup-Assistent für die Grundkonfiguration verschließt automatisch den Fernkonfigurationszugang über ISDN und schützt Ihr Gerät so gegen unbefugte Konfiguration. Den ISDN-Fernkonfigurationszugang können Sie auf Wunsch jederzeit im Sicherheits-Assistenten ein- oder ausschalten (siehe 'Haben Sie die Fernkonfiguration zugelassen?' auf Seite 73).

3.1.3 Einstellungen für den DSL-Anschluss

Für den DSL-Anschluss kann die Angabe des verwendeten Übertragungsprotokolls erforderlich sein. Der Assistent nimmt die korrekte Einstellung für die wichtigsten DSL-Anbieter selbstständig vor. Nur wenn der Assistent Ihren Anbieter nicht aufführt, müssen Sie das von Ihrem DSL-Anbieter verwendete Übertragungsprotokoll angeben.

Der Assistent bietet Ihnen auch ein Universalprotokoll 'Multimode' an, das mit allen gängigen DSL-Anschlüssen funktioniert.

3.1.4 Einstellungen für den ISDN-Anschluss

Wenn Sie den ISDN-Anschluss verwenden möchten, können Sie folgende Einstellungen vornehmen:

- Eine oder mehrere ISDN-MSNs, an der der Router Anrufe entgegennehmen soll. MSNs sind ISDN-Rufnummern, die Ihnen vom Telefonanbieter zugewiesen werden. Sie werden normalerweise ohne Vorwahl angegeben. Die angegebenen Nummern haben nur für Router-Funktionen (LAN-

LAN-Kopplung, RAS) Bedeutung, nicht jedoch für die Fernkonfiguration und LANCOM VPN Option.

- Eine Amtsvorwahl für den Zugang zum öffentlichen Netz. Sie ist normalerweise nur beim Anschluss an einer ISDN-Telefonanlage erforderlich. Üblich ist die '0'. Diese Amtsvorwahl wird für alle ausgehenden Rufe verwendet.
- Schließlich sollten Sie wissen, ob die Telefongesellschaft den ISDN-Gebührenimpuls übermittelt. Dieser kann vom LANCOM für Gebührenbudgets und die Accounting-Funktion ausgewertet werden.

3.1.5 Gebührenschutz

Der Gebührenschutz verhindert den Verbindungsaufbau über ein vorher eingestelltes Maß hinaus und schützt Sie so vor unerwartet hohen Verbindungskosten.

Beim LANCOM existieren drei unabhängige Budgets: Für den DSL-Zugang können Sie eine maximale Verbindungszeit in Minuten festsetzen. Für die Beschränkung von ISDN-Verbindungen existiert neben einem solchen Zeitbudget auch ein Budget für Gebühreneinheiten.

Für das Funktionieren der Beschränkung nach Gebühreneinheiten ist die Übermittlung der Gebühreninformationen im ISDN notwendig.

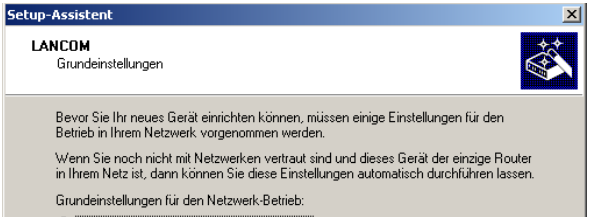
Jedes Budget kann durch Eingabe des Wertes '0' einzeln deaktiviert werden.

Auf Wunsch ist es möglich, den Gebührenschutz komplett auszuschalten.

3.2 Anleitung für LANconfig

① Starten Sie LANconfig mit **Start** ▶ **Programme** ▶ **LANCOM** ▶ **LANconfig**.

LANconfig erkennt den neuen LANCOM im TCP/IP-Netz selbstständig. Daraufhin startet der Setup-Assistent, der Ihnen bei der Grundeinstellung des Geräts behilflich ist oder Ihnen (die passende Netzwerkumgebung vorausgesetzt) sogar die gesamte Arbeit abnimmt.


Setup-Assistent
LANCOM
Grundeinstellungen
Bevor Sie Ihr neues Gerät einrichten können, müssen einige Einstellungen für den Betrieb in Ihrem Netzwerk vorgenommen werden.
Wenn Sie noch nicht mit Netzwerken vertraut sind und dieses Gerät der einzige Router in Ihrem Netz ist, dann können Sie diese Einstellungen automatisch durchführen lassen.
Grundeinstellungen für den Netzwerk-Betrieb:

Sollte der Setup-Assistent nicht automatisch starten, so suchen Sie manuell nach neuen Geräten an allen Schnittstellen (falls der LANCOM über die serielle Konfigurationsschnittstelle angeschlossen ist) oder im Netzwerk (**Gerät** ▶ **Suchen**).

Sollte der Zugriff auf einen unkonfigurierten LANCOM scheitern, so kann dieser Fehler auf die Netzmaske des LAN zurückzuführen sein: Bei weniger als 254 möglichen Hosts (Netzmaske > '255.255.255.0') muss sichergestellt sein, dass die IP-Adresse 'x.x.x.254' im eigenen Subnet vorhanden ist.

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ④ fort.

② Wenn Sie die TCP/IP-Einstellungen selber vornehmen wollen, dann geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Bestätigen Sie mit **Weiter**.

③ Geben Sie an, ob der Router als DHCP-Server arbeiten soll oder nicht. Wählen Sie aus, und bestätigen Sie mit **Weiter**.

④ Im folgenden Fenster legen Sie zunächst das Kennwort für den Konfigurationszugriff fest. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

Ferner legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf

achten, dass der Konfigurationszugriff durch ein Kennwort abgesichert ist.

⑤ Wählen Sie im nächsten Fenster Ihren DSL-Anbieter aus der angebotenen Liste aus. Bei Auswahl von 'Mein Anbieter ist hier nicht aufgeführt' müssen Sie das von Ihrem DSL-Anbieter verwendete Übertragungsprotokoll manuell angeben. In aller Regel funktioniert das Universal-Protokoll 'Multimode'. Bestätigen Sie mit **Weiter**.

⑥ Geben Sie diejenigen ISDN-Rufnummern (in Form von MSNs, also ohne Vorwahl) an, auf denen der Router Rufe annehmen soll. Mehrere Nummern werden durch Semikola getrennt. Wenn Sie keine MSN angegeben, reagiert der Routern auf alle Anrufe am ISDN-Anschluss.

Außerdem können Sie eine Amtsziffer für die Wahl ins ISDN eingeben. Schließlich sollten Sie angeben, ob an Ihrem ISDN-Anschluss die Gebühreninformationen übermittelt werden oder nicht. Bestätigen Sie mit **Weiter**.

⑦ Der Gebührenschutz beschränkt auf Wunsch die Kosten von DSL- und ISDN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Weiter**.

⑧ Schließen Sie die Konfiguration mit **Fertig stellen** ab.

Im Abschnitt 'TCP/IP-Einstellungen an den Arbeitsplatz-PCs' auf Seite 44 erfahren Sie, welche Einstellungen an den Arbeitsplatzrechnern im LAN notwendig sind.

3.3 Anleitung für WEBconfig

Für die Konfiguration mit WEBconfig müssen Sie wissen, wie sich der Router im LAN ansprechen lässt. Das Verhalten der Geräte sowie ihre Erreichbarkeit zur Konfiguration über einen Webbrowser hängen davon ab, ob im LAN schon DHCP-Server und DNS-Server aktiv sind, und ob diese beiden Serverprozesse die Zuordnung von IP-Adressen zu symbolischen Namen im LAN untereinander austauschen.

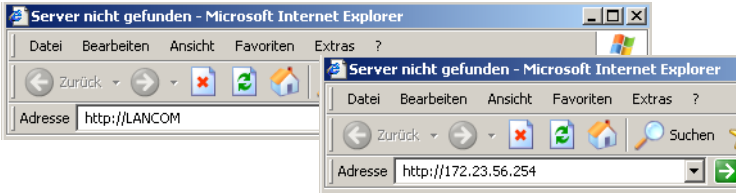
Nach dem Einschalten prüfen unkonfigurierte LANCOM-Geräte zunächst, ob im LAN schon ein DHCP-Server aktiv ist. Je nach Situation kann das Gerät dann den eigenen DHCP-Server einschalten oder alternativ den DHCP-Client-

DE

Modus aktivieren. In dieser zweiten Betriebsart kann das Gerät selbst eine IP-Adresse von einem im LAN schon vorhandenen DHCP-Server beziehen.

Netz ohne DHCP-Server

In einem Netz ohne DHCP-Server schalten unkonfigurierte LANCOM-Geräte nach dem Starten den eigenen DHCP-Serverdienst ein und weisen den anderen Rechner im LAN die IP-Adressen sowie Informationen über Gateways etc. zu, sofern diese auf den automatischen Bezug der IP-Adressen eingestellt sind (Auto-DHCP). In dieser Konstellation kann das Gerät von jedem Rechner mit aktivierter Auto-DHCP-Funktion mit einem Webbrowser unter dem Namen **LANCOM** oder unter der IP-Adresse **172.23.56.254** erreicht werden.



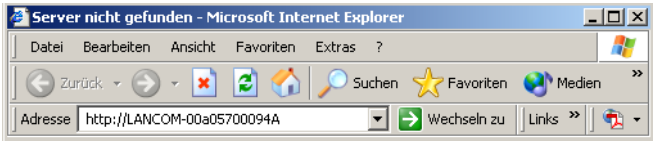
Falls der Konfigurations-Rechner seine IP-Adresse nicht vom LANCOM-DHCP-Server bezieht, ermitteln Sie die aktuelle IP-Adresse des Rechners (mit **Start** ▶ **Ausführen** ▶ **cmd** und dem Befehl **ipconfig** an der Eingabeaufforderung unter Windows 2000 oder Windows XP, mit **Start** ▶ **Ausführen** ▶ **cmd** und dem Befehl **winipcfg** an der Eingabeaufforderung unter Windows Me oder Windows 9x bzw. dem Befehl **ifconfig** in der Konsole unter Linux). In diesem Fall erreichen Sie das LANCOM unter der Adresse **x.x.x.254** (die "x" stehen für die ersten drei Blöcke in der IP-Adresse des Konfigurationsrechners).

Netz mit DHCP-Server

Ist im LAN ein DHCP-Server zur Zuweisung der IP-Adressen aktiv, schaltet ein unkonfiguriertes LANCOM-Gerät seinen eigenen DHCP-Server aus, wechselt in den DHCP-Client-Modus und bezieht eine IP-Adresse vom DHCP-Server aus dem LAN. Diese IP-Adresse ist aber zunächst nicht bekannt, die Erreichbarkeit des Geräts hängt von der Namensauflösung ab:

- Ist im LAN auch ein DNS-Server zur Auflösung der Namen vorhanden und tauscht dieser die Zuordnung von IP-Adressen zu den Namen mit dem

DHCP-Server aus, kann das Gerät unter dem Namen "LANCOM-<MAC-Adresse>" (z.B. "LANCOM-00a057xxxxxx") erreicht werden.



Die MAC-Adresse finden Sie auf einem Aufkleber auf der Geräteunterseite.

- Ist im LAN kein DNS-Server vorhanden oder ist dieser nicht mit dem DHCP-Server gekoppelt, kann das Gerät nicht über den Namen erreicht werden. In diesem Fall bleiben folgende Optionen:
  - Die per DHCP an das LANCOM-Gerät zugewiesene IP-Adresse über geeignete Tools ausfindig machen und das Gerät mit dieser IP-Adresse direkt erreichen.
  - LANconfig verwenden.
  - Einen Rechner mit Terminalprogramm über die serielle Konfigurationsschnittstelle an das Gerät anschliessen.

Aufruf der Assistenten in WEBconfig

① Öffnen Sie also Ihren Web-Browser (z. B. Internet Explorer, Netscape Navigator, Opera) und rufen Sie dort den LANCOM auf:

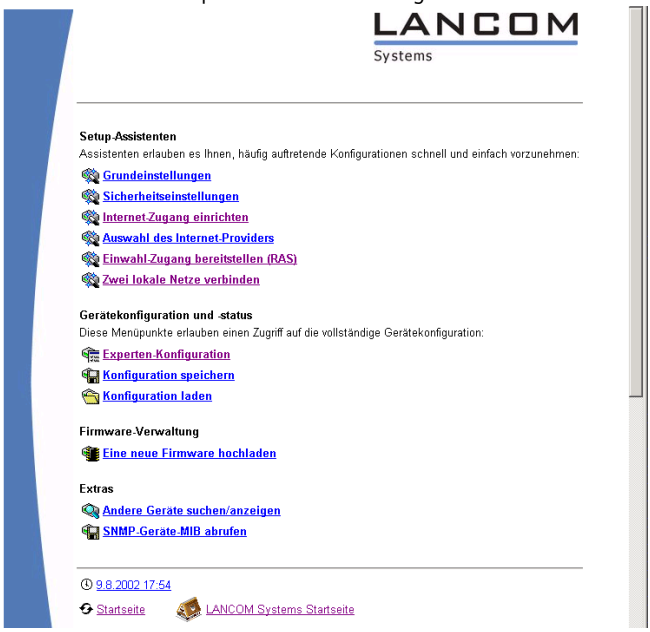
```
http://<IP-Adresse des LANCOM>
```

(bzw. über Namen wie oben beschrieben)

Sollte der Zugriff auf einen unkonfigurierten LANCOM scheitern, so kann dieser Fehler auf die Netzmaske des LAN zurückzuführen sein: Bei weniger als 254 möglichen Hosts (Netzmaske > '255.255.255.0') muss sichergestellt sein, dass die IP-Adresse 'x.x.x.254' im eigenen Subnet vorhanden ist.

DE

Es erscheint das Hauptmenü von WEBconfig:



Die Setup-Assistenten sind exakt auf die Funktionalität des jeweiligen LANCOM zugeschnitten. Es kann daher sein, dass Ihr Gerät nicht alle hier abgebildeten Assistenten anbietet.

Wenn Sie die automatische TCP/IP-Konfiguration wählen, fahren Sie mit Schritt ③ fort.

② Wenn Sie die TCP/IP-Einstellungen selber vornehmen wollten, dann geben Sie dem LANCOM eine verfügbare Adresse aus einem geeigneten IP-Adressbereich. Stellen Sie außerdem ein, ob er als DHCP-Server arbeiten soll oder nicht. Bestätigen Sie Ihre Eingabe mit **Setzen**.

③ Im folgenden Fenster 'Sicherheitseinstellungen' vergeben Sie zunächst ein Kennwort für den Konfigurationszugriff. Achten Sie bei der Eingabe auf Groß- und Kleinschreibung, sowie auf eine ausreichende Länge (mindestens 6 Zeichen).

Legen Sie fest, ob das Gerät nur aus dem lokalen Netzwerk heraus konfiguriert werden darf, oder ob auch die Fernkonfiguration über das WAN (also aus einem entfernten Netzwerk) erlaubt ist.

Bitte beachten Sie, dass mit dieser Freigabe auch die Fernkonfiguration über das Internet ermöglicht wird. Sie sollten in jedem Fall darauf achten, dass der Konfigurationszugriff geeignet abgesichert ist, z. B. durch ein Kennwort.

Unabhängig von der WAN-Fernkonfiguration ist die Fernkonfiguration über eine direkte ISDN-Verbindung: Hier wählt sich der Konfigurations-PC direkt über ISDN (beispielsweise über das DFÜ-Netzwerk von Windows) in den LANCOM ein. Durch die Angabe einer MSN/EAZ aktivieren Sie die ISDN-Fernkonfiguration. In diesem Fall nimmt der LANCOM Anrufe an der angegebenen MSN/EAZ entgegen und kann über die aufgebaute Verbindung konfiguriert werden.

Bestätigen Sie Ihre Wahl mit **Setzen**.

④ Wählen Sie im nächsten Fenster Ihren DSL-Anbieter aus der angebotenen Liste aus. Bestätigen Sie Ihre Wahl mit **Setzen**.

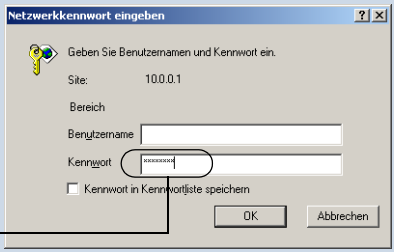
Bei Auswahl von 'Mein Anbieter ist hier nicht aufgeführt' müssen Sie im anschließenden Fenster das von Ihrem DSL-Anbieter verwendete Übertragungsprotokoll manuell angeben. In aller Regel funktioniert das Universal-Protokoll 'Multimode'.

⑤ Der Gebührenschutz beschränkt auf Wunsch die Kosten von DSL- und ISDN-Verbindungen auf ein festgesetztes Maß. Bestätigen Sie Ihre Angaben mit **Setzen**.

Wenn Ihr Gerät über keine ISDN-Schnittstelle verfügt, können Sie den Setup-Assistenten jetzt fertig stellen. Ansonsten bietet Ihnen der Assistent

Eingabe des Kennworts im Web-Browser

Wenn Sie künftig beim Zugriff auf das Gerät von Ihrem Web-Browser zur Eingabe des Kennworts aufgefordert werden, tragen Sie dieses im Feld **Kennwort** ein. Achten Sie auf Groß- und Kleinschreibung. Das Feld **Benutzername** bleibt leer.



Eingabe des Konfigurations-Kennworts

an, abschließend die ISDN-Schnittstelle zu konfigurieren. Treffen Sie eine Wahl und bestätigen Sie mit **Setzen**.

⑥ Geben Sie diejenigen ISDN-Rufnummern (in Form von MSNs, also ohne Vorwahl) an, auf denen der Router Rufe annehmen soll. Mehrere Nummern werden durch Semikola getrennt. Wenn Sie keine MSN angegeben, reagiert der Routern auf alle Anrufe am ISDN-Anschluss.

Außerdem können Sie eine Amtsziffer für die Wahl ins ISDN eingeben. Schließlich sollten Sie angeben, ob an Ihrem ISDN-Anschluss die Gebühreninformationen übermittelt werden oder nicht. Bestätigen Sie Ihre Eingaben mit **Setzen**.

⑦ Der Grundeinrichtungs-Assistent meldet, dass alle notwendigen Angaben vorliegen. Mit **Weiter** schließen Sie ihn ab.

3.4 TCP/IP-Einstellungen an den Arbeitsplatz-PCs

Bei TCP/IP-Netzwerken ist die korrekte Adressierung aller Geräte im LAN außerordentlich wichtig. Ferner sollten alle Rechner die IP-Adressen von zwei zentralen Stellen im LAN kennen:

- Standard-Gateway – erhält alle Pakete, die nicht an Rechner im lokalen Netz adressiert sind
- DNS-Server – übersetzt einen Netzwerknamen (www.**lancom.de**) oder den Namen eines Rechners (**www**.lancom.de) in eine konkrete IP-Adresse.

Der LANCOM kann sowohl die Funktionen eines Standard-Gateways als auch die eines DNS-Servers übernehmen. Außerdem kann er als DHCP-Server allen Rechnern im LAN automatisch eine korrekte IP-Adresse zuweisen.

Die korrekte TCP/IP-Konfiguration der PC im LAN hängt entscheidend davon ab, nach welcher Methode im LAN die IP-Adressen vergeben werden:

- **IP-Adressvergabe über den LANCOM (Normalfall)**

  In dieser Betriebsart weist der LANCOM den PCs im LAN nicht nur eine IP-Adresse zu, sondern übermittelt per DHCP auch seine eigene IP-Adresse als Standard-Gateway und DNS-Server. Die PCs sind deshalb so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server automatisch (über DHCP) beziehen.

- **IP-Adressvergabe über einen separaten DHCP-Server**

  Die Arbeitsplatz-PCs sind so einzustellen, dass sie ihre eigene IP-Adresse, ebenso wie die IP-Adressen von Standard-Gateway und DNS-Server auto-

matisch (über DHCP) beziehen. Auf dem DHCP-Server ist die IP-Adresse des LANCOM so zu hinterlegen, dass der DHCP-Server sie an die PCs im LAN als Standard-Gateway übermittelt. Außerdem sollte der DHCP-Server den LANCOM als DNS-Server angeben.

- **Manuelle Zuweisung der IP-Adressen**

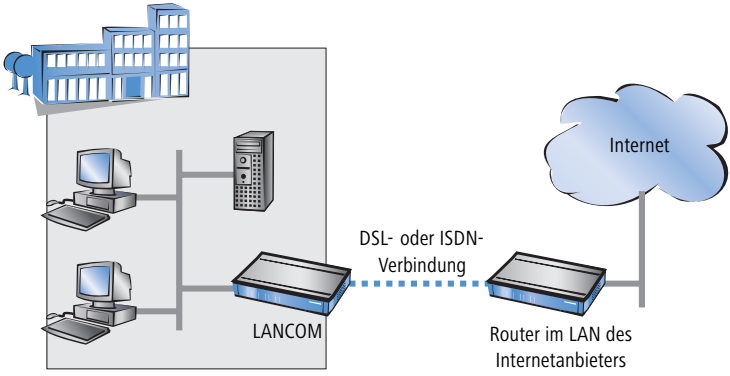
  Werden die IP-Adressen im Netzwerk statisch vergeben, so sind bei jedem PC im LAN die IP-Adresse des LANCOM als Standard-Gateway und als DNS-Server in der TCP/IP-Konfiguration einzustellen.

Weitere Informationen und Hilfe zu den TCP/IP-Einstellungen Ihres LANCOM finden Sie im Referenzhandbuch. Bei der Netzwerkkonfiguration der Arbeitsplatzrechner hilft Ihnen die Dokumentation des installierten Betriebssystems weiter.

DE

4 Den Internet-Zugang einrichten

Über den zentralen Internet-Zugang des LANCOM erhalten alle Rechner im LAN Zugriff auf das Internet. Die Verbindung zum Internetanbieter kann über jeden WAN-Anschluss aufgebaut werden. Ein Internet-Zugang über ISDN kann beispielsweise als Backup für DSL eingesetzt werden.



Kennt der Setup-Assistent Ihren Internet-Anbieter?

Die Einrichtung des Internet-Zugangs erfolgt über einen komfortablen Assistenten. Der Assistent kennt die Zugangsdaten der wichtigsten Internetanbieter und bietet Ihnen eine Liste zur Auswahl an. Wenn Sie Ihren Internetanbieter in dieser Liste finden, so müssen Sie für die Einrichtung des Internet-Zugangs normalerweise keine weiteren Übertragungs-Parameter eingeben. Lediglich die Authentifizierungsdaten, die Ihnen Ihr Internetanbieter zur Verfügung stellt, sind noch erforderlich.

Zusätzlich Angaben bei unbekanntem Internet-Anbieter

Kennt der Setup-Assistent Ihren Internet-Anbieter nicht, so fragt er Sie Schritt für Schritt alle notwendigen Zugangsdaten ab. Diese Zugangsdaten stellt Ihnen Ihr Internet-Anbieter zur Verfügung.

- **ADSL**
  - Protokoll: PPP (PPPoA), PPPoE, Plain IP (IPoA) oder Plain Ethernet
  - ATM-Parameter: VPI (Virtual Path Identifier) und VCI (Virtual Circuit Identifier). Außerdem Angabe der Encapsulation (VC- oder LLC-based Multiplexing)

- Zusätzlich bei Plain IP (IPoA) und Plain Ethernet: eigene öffentliche IP-Adresse mit Netzmaske (nicht zu verwechseln mit der privaten LAN-IP-Adresse), Default-Gateway und DNS-Server. Wenn der Provider DHCP unterstützt, können diese IP-Parameter automatisch bezogen werden.

- **DSL**
  - Protokoll: PPPoE, PPTP oder Plain Ethernet (IPoE oder IPoEoA)
  - Zusätzlich bei Plain Ethernet: eigene öffentliche IP-Adresse mit Netzmaske (nicht zu verwechseln mit der privaten LAN-IP-Adresse), Default-Gateway und DNS-Server. Wenn der Provider DHCP unterstützt, können diese IP-Parameter automatisch bezogen werden.
  - Benutzername und Passwort
- **ISDN**
  - Einwahlrufnummer
  - Benutzername und Passwort

Weitere Verbindungsoptionen

Zusätzlich können Sie (sofern von Ihrem Internetanbieter unterstützt) zusätzliche Optionen im Assistenten ein- oder ausschalten:

- Zeitliche Abrechnung oder Flatrate – wählen Sie aus, nach welchem Modell Ihr Internetanbieter die Nutzung abrechnet.
  - Bei der zeitlichen Abrechnung können Sie am LANCOM einstellen, dass bestehende Verbindungen automatisch abgebaut werden, wenn für eine bestimmte Dauer (die sogenannte Haltezeit) keine Daten mehr übertragen wurden.

    Zusätzlich können Sie eine Leitungsüberwachung aktivieren, die inaktive Gegenstellen schneller erkennt und in diesem Fall die Verbindung schon vor Ablauf der Haltezeit abbaut.
  - Bei Flatrate-Abrechnung haben Sie ebenfalls die Möglichkeit der aktiven Leitungsüberwachung, und können so die Funktion der Gegenstelle ständig überprüfen.

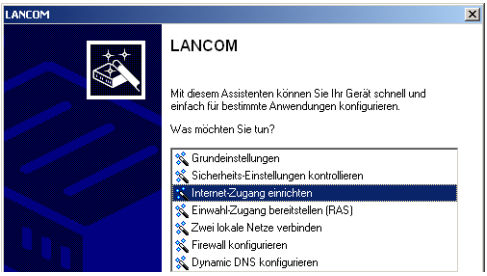
    Außerdem können Sie bei Flatrates Verbindungen dauerhaft aufrecht erhalten („Keep-alive"). Im Fall eines Verbindungsabbruchs wird diese automatisch wieder aufgebaut.
- Dynamische Kanalbündelung (nur ISDN)
  - Bei Bedarf wird automatisch der zweite ISDN-B-Kanal zur Verbindung hinzugeschaltet. Dadurch wird die Bandbreite verdoppelt. Unter

Umständen werden aber auch die doppelten Verbindungsgebühren fällig. Außerdem ist Ihr ISDN-Anschluss in diesem Fall besetzt, zusätzliche ein- oder ausgehende Anrufe werden abgelehnt.

- Datenkompression
  - Sie ermöglicht eine zusätzliche Steigerung der Übertragungsgeschwindigkeit.

4.1 Anleitung für LANconfig

① Markieren Sie Ihr LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Internet-Zugang einrichten** und bestätigen Sie die Auswahl mit **Weiter**.

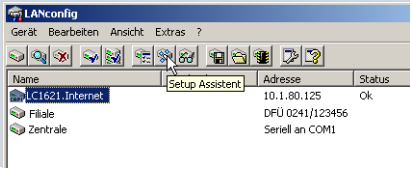
③ In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.

④ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.

⑤ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

LANconfig:
Schneller Aufruf der Setup-Assistenten

Die Setup-Assistenten rufen Sie unter LANconfig am schnellsten über den Befehlsknopf in der Button-Leiste auf.



4.2 Anleitung für WEBconfig

① Wählen Sie im Hauptmenü **Internet-Zugang einrichten**.

② In den folgenden Fenstern wählen Sie Ihr Land, nach Möglichkeit Ihren Internetanbieter, und geben Sie die Zugangsdaten ein.

③ Je nach Verfügbarkeit bietet Ihnen der Assistent weitere Optionen für die Internetverbindung zur Auswahl an.

④ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Weiter** ab.

5 Zwei Netzwerke verbinden

Mit der Netzwerkkopplung (auch LAN-LAN-Kopplung) des LANCOM werden zwei lokale Netzwerke miteinander verbunden. Die LAN-LAN-Kopplung kann grundsätzlich auf zwei verschiedenen Wegen realisiert werden:

DE

Nur LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN

- **VPN**: Bei der Kopplung über VPN wird die Verbindung zwischen den beiden LANs über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. In beiden LANs wird dazu ein Router mit VPN-Unterstützung benötigt.
- **ISDN**: Bei der Kopplung über ISDN wird eine direkt Verbindung zwischen den beiden LANs über eine ISDN-Verbindung hergestellt. In beiden LANs wird ein dazu Router mit ISDN-Schnittstelle benötigt.

Die Einrichtung einer LAN-LAN-Kopplung erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Immer beide Seiten konfigurieren

Beide an der Netzwerkkopplung beteiligten Router müssen konfiguriert werden. Dabei ist darauf zu achten, dass die Konfigurationsangaben auf beiden Seiten zueinander passen.

Die folgende Anleitung geht davon aus, dass auf beiden Seiten LANCOM-Router verwendet werden. Die Netzwerkkopplung ist zwar auch mit Routern anderer Hersteller möglich. Eine gemischte Konfiguration erfordert aber in aller Regel tiefer gehende Eingriffe an beiden Geräten. Ziehen Sie in einem solchen Fall das Referenzhandbuch zu Rate.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein. Ein LANCOM bietet daher eine ganze Reihe von Sicherheitsmechanismen an, bei deren Einsatz ein hervorragender Schutz gewährleistet ist:

- **VPN**: Bei Kopplungen über VPN werden die Daten mittels IPSec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt
- **ISDN**: Bei Kopplungen über ISDN sorgen das Kennwort für die Verbindung, die Überprüfung der ISDN-Nummer und die Rückruffunktion für die Sicherheit der Verbindung.

Die ISDN-Rückruffunktion kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

5.1 Welche Angaben sind notwendig?

Der Assistent fragt alle notwendigen Daten Schritt für Schritt ab. Nach Möglichkeit sollten Ihnen die erforderlichen Angaben schon vor Aufruf des Assistenten vorliegen.

Die Bedeutung aller Angaben, nach denen Sie der Assistent fragt, erklären wir Ihnen an Hand eines typischen Beispiels: der Kopplung einer Filiale an ihre Zentrale. Die beiden beteiligten Router tragen die Namen 'ZENTRALE' und 'FILIALE'.

Den folgenden Tabellen entnehmen Sie, welche Einträge an welchem der beiden Router vorzunehmen sind. Pfeile kennzeichnen die Abhängigkeiten zwischen den Einträgen.

5.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung einer LAN-LAN-Kopplung benötigt. Die erste Spalte zeigt jeweils an, ob die Information für eine VPN und/oder ISDN-Netzwerkkopplung erforderlich ist.

Kopplung	Angabe	Gateway 1		Gateway 2
VPN	Verfügt die Gegenstelle über einen ISDN-Anschluss?	Ja/Nein		Ja/Nein
VPN	Typ der eigenen IP-Adresse	statisch/dynamisch	⤫	statisch/dynamisch
VPN	Typ IP-Adresse der Gegenstelle	statisch/dynamisch		statisch/dynamisch
VPN + ISDN	Name des eigenen Gerätes	'ZENTRALE'	⤫	'FILIALE'
VPN + ISDN	Name der Gegenstelle	'FILIALE'		'ZENTRALE'
VPN + ISDN	ISDN-Rufnummer Gegenstelle	(0123) 123456	⤫	(0789) 654321
VPN + ISDN	ISDN-Anruferkennung Gegenstelle	(0789) 654321		(0123) 123456
VPN + ISDN	Kennwort zur sicheren Übertragung der IP-Adresse	'Geheim'	↔	'Geheim'
VPN	Shared Secret für Verschlüsselung	'Secret'	↔	'Secret'
VPN	IP-Adresse der Gegenstelle	'10.0.2.100'		'10.0.1.100'

Kopplung	Angabe	Gateway 1		Gateway 2
VPN	IP-Netzadresse des entfernten Netzes	'10.0.2.0'		'10.0.1.0'
VPN	Netzmaske des entfernten Netzwerks	255.255.255.0		255.255.255.0
VPN	Dömänenbezeichnung im entfernten Netzwerk	'zentrale'		'filiale'
VPN	Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)?	Ja/Nein		Ja/Nein
ISDN	TCP/IP-Routing für Zugriff auf entferntes Netz?	Ja/Nein		Ja/Nein
ISDN	IPX-Routing für Zugriff auf entferntes Netz?	Ja/Nein		Ja/Nein
VPN + ISDN	NetBIOS-Routing für Zugriff auf entferntes Netz?	Ja/Nein		Ja/Nein
VPN + ISDN	Name einer lokalen Arbeitsgruppe (nur bei NetBIOS)	'workgroup1'		'workgroup2'
ISDN	Datenkomprimierung	ein/aus	⟷	ein/aus
ISDN	Kanalbündelung	ein/aus	⟷	ein/aus

Hinweise zu den einzelnen Werten:

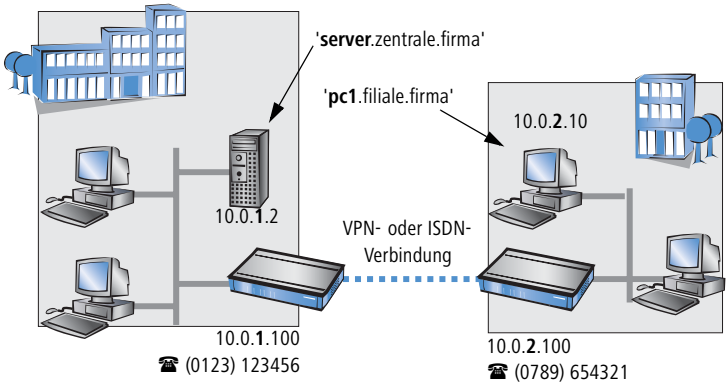
- Verfügt Ihr eigenes Gerät über einen **ISDN-Anschluss**, so fragt der Assistent nach, ob auch die Gegenstelle über einen solchen verfügt.
- Für VPN-Verbindungen über das Internet muss der Typ der IP-Adressen auf beiden Seiten angegeben werden. Es gibt zwei **Typen von IP-Adressen**: statische und dynamische. Eine Erklärung zum Unterschied der beiden IP-Adresstypen finden Sie im Referenzhandbuch.

  Die Dynamic-VPN-Funktionalität erlaubt VPN-Verbindungen nicht nur zwischen Gateways mit statischen (festen) IP-Adressen, sondern auch bei Verwendung dynamischer IP-Adressen. Der aktive Aufbau von VPN-Verbindungen zu Gegenstellen mit dynamischer IP-Adresse erfordert eine ISDN-Verbindung.
- Wenn Sie Ihren LANCOM noch nicht benannt haben, so fragt Sie der Assistent nach einem neuen **eigenen Gerätenamen.** Mit der Eingabe benennen Sie Ihren LANCOM neu. Achten Sie darauf, dass Sie beide Gegenstellen unterschiedlich benennen.
- Der **Name der Gegenstelle** wird für deren Identifikation benötigt.
- Im Feld **ISDN-Rufnummer** wird die Rufnummer der ISDN-Gegenstelle angegeben. Erforderlich ist die Angabe der kompletten Rufnummer der Gegenstelle einschließlich aller notwendigen Vorwahlen.

- Mit der angegebenen **ISDN-Anruferkennung** wird der Anrufer identifiziert und authentifiziert. Wird ein LANCOM angerufen, vergleicht er die für die Gegenstelle eingetragene ISDN-Anruferkennung mit der Kennung, die der Anrufer tatsächlich über den D-Kanal übermittelt. Eine ISDN-Kennung setzt sich üblicherweise aus der nationalen Vorwahl und einer MSN zusammen.
- Das **Kennwort für die ISDN-Verbindung** ist eine Alternative zur ISDN-Anruferkennung. Es wird immer dann zur Authentifizierung des Anrufers herangezogen, wenn keine ISDN-Anruferkennung übermittelt wird. Das Kennwort muss auf beiden Seiten identisch eingegeben werden. Es wird für Anrufe in beide Richtungen verwendet.
- Das **Shared Secret** ist das zentrale Kennwort für die Sicherheit der VPN-Verbindung. Es muss auf beiden Seiten identisch eingegeben werden.
- Die Datenkomprimierung erhöht die Übertragungsgeschwindigkeit ohne zusätzliche Kosten. Ganz im Gegensatz zur Bündelung von zwei ISDN-Kanälen mit MLPPP (**M**ulti**L**ink-**PPP**): Hier wird zwar die Bandbreite verdoppelt, in aller Regel fallen dafür aber auch doppelte Verbindungsgebühren an.

5.1.2 Einstellungen für den TCP/IP-Router

Im TCP/IP-Netzwerk kommt der korrekten Adressierung eine besondere Bedeutung zu. Bei einer Netzwerkkopplung ist zu beachten, dass beide Netzwerke logisch voneinander getrennt sind. Sie müssen daher jeweils über eine eigene Netzwerknummer verfügen (im Beispielfall '10.0.1.x' und '10.0.2.x'). Die beiden Netzwerknummern müssen unterschiedlich sein.



LAN der Zentrale. IP: 10.0.**1.0**,
Netzmaske: 255.255.255.0
Domäne: '**zentrale**.firma'

LAN der Filiale. IP: 10.0.**2.0**,
Netzmaske: 255.255.255.0
Domäne: '**filiale**.firma'

Im Gegensatz zum Internet-Zugang werden bei der Kopplung von Netzen alle IP-Adressen aus den beteiligten Netzen auch im entfernten LAN sichtbar, nicht nur die der Router. Der Rechner mit der IP-Adresse 10.0.2.10 im LAN der Filiale sieht den Server 10.0.1.2 in der Zentrale und kann (entsprechende Rechte vorausgesetzt) auch auf ihn zugreifen. Gleiches gilt umgekehrt.

DNS-Zugriffe ins entfernte LAN

Der Zugriff auf entfernte Rechner kann in einem TCP/IP-Netzwerk nicht nur über die Angabe der IP-Adresse erfolgen, sondern dank DNS auch über frei definierbare Namen.

Beispielsweise kann der Rechner mit dem Namen 'pc1.filiale.firma' (IP 10.0.2.10) auf den Server in der Zentrale nicht nur über dessen IP-Adresse zugreifen, sondern auch über dessen Namen 'server.zentrale.firma'. Einzige Voraussetzung: Die Domäne des entfernten Netzwerks muss im Assistenten angegeben werden.

Die Angabe der Domäne ist nur im LANconfig-Assistenten möglich. Bei WEBconfig nehmen Sie die entsprechenden Einstellungen später in der Expertenkonfiguration vor. Nähere Informationen finden Sie im LANCOM-Referenzhandbuch.

VPN-Extranet

Bei einer LAN-LAN-Kopplung über VPN können Sie die eigenen Stationen hinter einer anderen IP-Adresse maskieren. Bei dieser als 'Extranet-VPN' bezeichneten Betriebsart erscheinen die eigenen Rechner gegenüber dem entfernten LAN nicht mit ihrer eigenen IP-Adresse, sondern mit einer anderen frei wählbaren (z. B. der des VPN-Gateways).

Den Stationen im entfernten LAN wird dadurch der direkte Zugriff auf die Rechner im eigenen LAN verwehrt. Wurde beispielsweise im LAN der Filiale für den Zugriff auf die Zentrale der Extranet-VPN-Modus hinter der IP-Adresse '10.10.2.100' eingestellt, und greift der Rechner '10.10.2.10' auf den Server '10.10.1.2' zu, so erscheint bei diesem eine Anfrage von der IP '10.10.2.100'. Die tatsächliche IP-Adresse des Rechners bleibt verborgen.

Wenn ein LAN im Extranet-Modus gekoppelt wird, so wird auf der Gegenseite nicht dessen tatsächliche (verborgene) LAN-Adresse angegeben, sondern die IP-Adresse, mit der das LAN nach außen hin auftritt (im Beispiel '10.10.2.100'). Die Netzmaske lautet in diesem Fall '255.255.255.255'.

5.1.3 Einstellungen für den IPX-Router

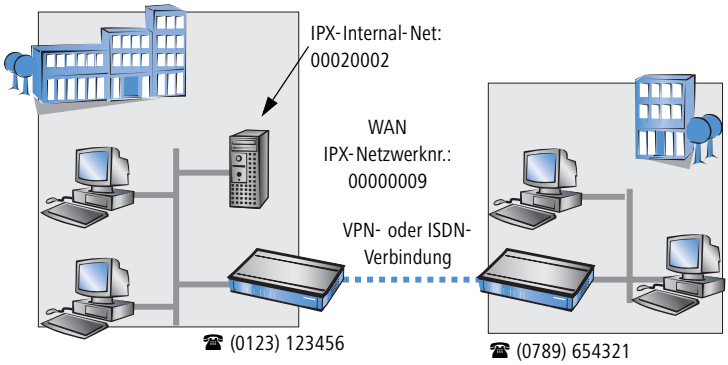
Die Kopplung von IPX-Netzwerken über VPN kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

Für die Kopplung von zwei typischen IPX-Netzwerken zu einem WAN sind drei IPX-Netzwerknummern notwendig:

- für das LAN der Zentrale
- für das LAN der Filiale
- für das übergeordnete WAN

Die IPX-Netzwerknummern in Zentrale und Filiale werden jeweils auf der entfernten Seite angegeben.

Die drei geforderten Netzwerknummern werden in den IPX-Konventionen als „External Network Numbers" bezeichnet. Sie gelten (ähnlich IP-Netzwerk-Adressen) für ein ganzes LAN-Segment. Im Gegensatz dazu dienen die IPX-Internal-Network-Nummern zur Adressierung eines bestimmten Novell-Servers im LAN. Alle drei angegebenen Netzwerknummern müssen sich voneinander und von allen verwendeten IPX-Internal-Network-Nummern unterscheiden.



Ferner kann die Angabe des im entfernten LAN verwendeten Frame-Typs („Binding") erforderlich sein.

Wenn im entfernten Netz ein Novell-Server arbeitet, ist die Angabe der entfernten IPX-Netzwerknummer und des verwendeten Bindings nicht erforderlich. In diesem Fall muss lediglich eine Netzwerknummer für das WAN manuell angegeben werden.

5.1.4 Einstellungen für NetBIOS-Routing

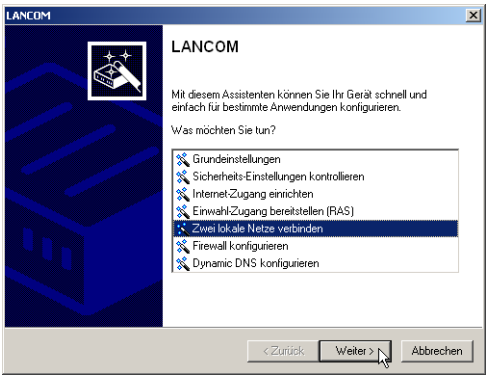
Das NetBIOS-Routing ist schnell eingerichtet: Zusätzlich zu den Angaben für das verwendete TCP/IP-Protokoll muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.

Entfernte Windows-Arbeitsgruppen erscheinen nicht in der Windows-Netzwerkumgebung, sondern können nur direkt (z. B. über die Computer-Suche) angesprochen werden.

5.2 Anleitung für LANconfig

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

① Rufen Sie den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie notwendigen Daten ein.



② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.

③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit `ping`) anzusprechen. Der LANCOM sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

5.3 Anleitung für WEBconfig

Die Kopplung von Netzwerken über VPN kann unter WEBconfig nicht mit Hilfe des Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

Führen Sie die Konfiguration nacheinander an beiden Routern durch.

Ping – schneller Verbindungstest einer TCP/IP-Verbindung

Für den Test einer TCP/IP-Verbindung schicken Sie einfach ein `ping` von Ihrem Rechner an einen Rechner im entfernten Netz. Details zum Ping-Befehl finden Sie in der Dokumentation Ihres Betriebssystems.

IPX- und NetBIOS-Verbindungen testen Sie, indem Sie von Ihrem Rechner aus einen entfernten Novell-Server bzw. einen Rechner in der entfernten Win-

Eingabeaufforderung
C:\>ping 10.0.1.2
Ping wird ausgeführt für 10.0.1.2 mit 32 Byte
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms TTL=
Antwort von 10.0.1.2: Bytes=32 Zeit=20ms TTL=
Antwort von 10.0.1.2: Bytes=32 Zeit=10ms TTL=
Antwort von 10.0.1.2: Bytes=32 Zeit<10ms TTL=
Ping-Statistik für 10.0.1.2:

① Rufen Sie im Hauptmenü den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.

② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Weiter** ab.

③ Nach Abschluss der Einrichtung an beiden Routern können Sie die Netzwerkverbindung testen. Versuchen Sie dazu, einen Rechner im entfernten LAN (z. B. mit `ping`) anzusprechen. Der LANCOM sollte automatisch eine Verbindung zur Gegenstelle aufbauen und den Kontakt zum gewünschten Rechner herstellen.

6 Einwahl-Zugang bereitstellen

An Ihrem LANCOM können Sie Einwahl-Zugänge einrichten, über die sich einzelne Rechner in Ihr LAN einwählen können und für die Dauer der Verbindung vollwertiger Teilnehmer des Netzwerks werden. Dieser Dienst wird auch als RAS (**R**emote **A**ccess **S**ervice) bezeichnet. Der RAS-Zugang kann grundsätzlich auf zwei verschiedenen Wegen realisiert werden:

Nur LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN

- **VPN**: Bei einem RAS-Zugang über VPN wird die Verbindung zwischen dem LAN und dem Einwahlrechner über eine besonders geschützte Verbindung über das öffentliche Internet hergestellt. Der Router im LAN benötigt eine VPN-Unterstützung, der Einwahlrechner einen beliebigen Zugang zum Internet und einen LANCOM VPN Client.
- **ISDN**: Bei einem RAS-Zugang über ISDN wird eine direkt Verbindung zwischen dem LAN und dem Einwahlrechne über eine ISDN-Verbindung hergestellt. Der Router im LAN benötigt eine ISDN-Schnittstelle, der Einwahlrechner einen ISDN-Adapter oder ein ISDN-Modem. Als Protokoll für die Datenübertragung dient PPP. Damit ist die Unterstützung aller üblichen Geräte und Betriebssysteme gesichert.

Die Einrichtung eines Einwahl-Zugangs erfolgt über einen Setup-Assistenten in bekannt komfortabler Art.

Sicherheitsaspekte

Der Zugang zu Ihrem LAN muss natürlich gegen unbefugten Zugriff geschützt sein. Ein LANCOM bietet daher eine ganze Reihe von Sicherheitsmechanismen an, bei deren Einsatz ein hervorragender Schutz gewährleistet ist:

- **VPN**: Bei Kopplungen über VPN werden die Daten mittels IPSec übertragen und dabei mit den Verfahren 3-DES, AES oder Blowfish verschlüsselt
- **ISDN**: Bei Kopplungen über ISDN sorgen das Kennwort für die Verbindung, die Überprüfung der ISDN-Nummer und die Rückruffunktion für die Sicherheit der Verbindung.

Die ISDN-Rückruffunktion kann nicht im Assistenten, sondern nur in der Expertenkonfiguration eingerichtet werden. Details dazu finden Sie im Referenzhandbuch.

6.1 Welche Angaben sind notwendig?

Der Assistent richtet den Einwahl-Zugang nur für einen Benutzer ein. Für jeden zusätzlichen Benutzer führen Sie den Assistenten ein weiteres Mal aus.

6.1.1 Allgemeine Angaben

Die folgenden Angaben werden für die Einrichtung eines RAS-Zugangs benötigt. Die erste Spalte zeigt jeweils an, ob die Information für einen VPN und/oder ISDN-Zugang erforderlich ist.

Kopplung	Angabe
VPN + ISDN	Benutzername
VPN + ISDN	Passwort
VPN	Shared Secret für Verschlüsselung
VPN	Eigene Stationen bei Zugriff auf entferntes Netz verstecken (Extranet-VPN)?
ISDN	Ankommende Rufnummer des Einwahlrechners
ISDN	TCP/IP-Routing für Zugriff auf entferntes Netz?
ISDN	IPX-Routing für Zugriff auf entferntes Netz?
VPN + ISDN	IP-Adresse(n) für den oder die Einwahlrechner: fest oder dynamisch aus einem Adressbereich (IP-Adress-Pool)
VPN + ISDN	NetBIOS-Routing für Zugriff auf entferntes Netz?
VPN + ISDN	Name einer lokalen Arbeitsgruppe (nur bei NetBIOS)

Hinweise zu den einzelnen Werten:

- **Benutzername und Passwort**: Mit diesen Zugangsdaten weist sich der Benutzer bei der Einwahl aus.
- **Ankommende Nummer**: Die optionale ISDN-Anruferkennung verwendet der LANCOM zusätzlich zur Benutzer-Authentifikation. Auf die Verwendung dieser Sicherheitsfunktion sollte immer dann verzichtet werden, wenn sich der Benutzer von verschiedenen ISDN-Anschlüssen einwählt.

Hinweise zu den anderen Werten, die bei der Einrichtung des RAS-Zugangs benötigt werden, finden Sie im Kapitel 'Zwei Netzwerke verbinden' auf Seite 50.

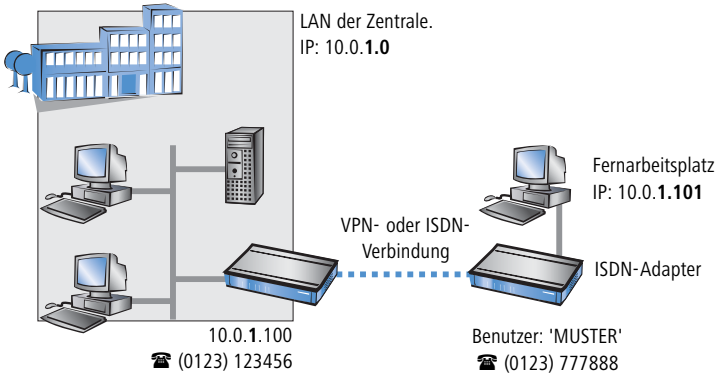
Die ISDN-Anruferkennung (CLI)

Bei der ISDN-Anruferkennung – auch als CLI (**C**alling **L**ine **I**dentity) bezeichnet – handelt sich um die Telefonnummer des Anrufers, die an den angerufenen Teilnehmer übermittelt wird. Sie setzt sich in aller Regel aus der nationalen Vorwahl und einer MSN zusammen.

Die CLI eignet sich aus zwei Gründen besonders gut für die Authentifizierung: Zum einen lässt sie sich nur schwer manipulieren. Zum anderen erfolgt ihre Übertragung kostenlos über den ISDN-Steuerkanal (D-Kanal).

6.1.2 Einstellungen für TCP/IP

Beim Protokoll TCP/IP muss jedem aktiven RAS-Benutzer eine eigene IP-Adresse zugewiesen werden.



Diese IP-Adresse können Sie entweder bei der Anlage eines Benutzers manuell festlegen. Einfacher ist es, den LANCOM einem Benutzer automatisch bei der Einwahl eine freie IP-Adresse zuteilen zu lassen. In diesem Fall legen Sie bei der Konfiguration nur den IP-Adressbereich fest, aus dem der LANCOM die Adresse für den RAS-Benutzer nehmen soll.

Achten Sie sowohl bei der manuellen als auch bei der automatischen IP-Adresszuteilung darauf, dass es sich um freie Adresse(n) aus dem Adressbereich Ihres lokalen Netzwerks handelt. Im Beispiel wird dem PC bei der Einwahl die IP-Adresse '10.0.1.101' zugewiesen.

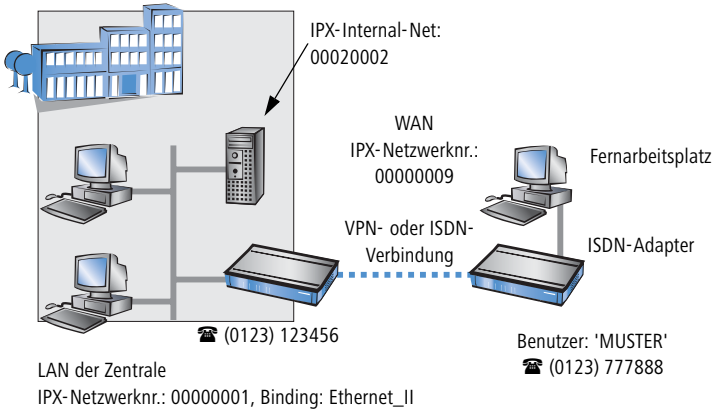
Mit dieser IP-Adresse ist der Rechner ein vollwertiger Teilnehmer im LAN: Er kann (bei entsprechender Berechtigung) auf alle anderen Geräte im LAN zugreifen. Umgekehrt gilt dieses Verhältnis auch: auf den entfernten Rechner kann auch aus dem LAN zugegriffen werden.

DE

6.1.3 Einstellungen für IPX

Für die RAS-Einwahl in ein IPX-Netzwerk ist die Angabe von zwei IPX-Netzwerknummern notwendig:

- die IPX-Netzwerknummer der Zentrale
- eine zusätzliche IPX-Netzwerknummer für das übergeordnete WAN



Die geforderten Netzwerknummern werden in den IPX-Konventionen als „External Network Numbers" bezeichnet. Sie gelten (analog zu IP-Netzwerk-Adressen) für ein komplettes LAN-Segment. Im Gegensatz dazu dienen die IPX-Internal-Network-Nummern zur Adressierung von bestimmten Novell-Servern im LAN. Alle drei angegebenen Netzwerknummern müssen sich voneinander und von allen verwendeten IPX-Internal-Network-Nummern unterscheiden.

Ferner kann die Angabe des im entfernten LAN verwendeten Frame-Typs („Binding") erforderlich sein.

Wenn im entfernten Netz ein Novell-Server arbeitet, ist die Angabe der entfernten IPX-Netzwerknummer und des verwendeten Bindings nicht erforderlich. Eine Netzwerknummer für das WAN muss allerdings auch in diesem Fall manuell angegeben werden.

6.1.4 Einstellungen für NetBIOS-Routing

Für die Verwendung von NetBIOS muss lediglich der Name einer Windows-Arbeitsgruppe aus dem eigenen LAN des Routers angegeben werden.

Die Verbindung wird nicht automatisch aufgebaut. Der RAS-Benutzer muss bei Bedarf zunächst manuell eine Verbindung über das DFÜ-Netzwerk zum LANCOM herstellen. Bei bestehender Verbindung kann die Rechner im anderen Netz suchen und auf sie zugreifen (über **Suchen** ▶ **Computer**, nicht über die Netzwerkumgebung).

6.2 Einstellungen am Einwahl-Rechner

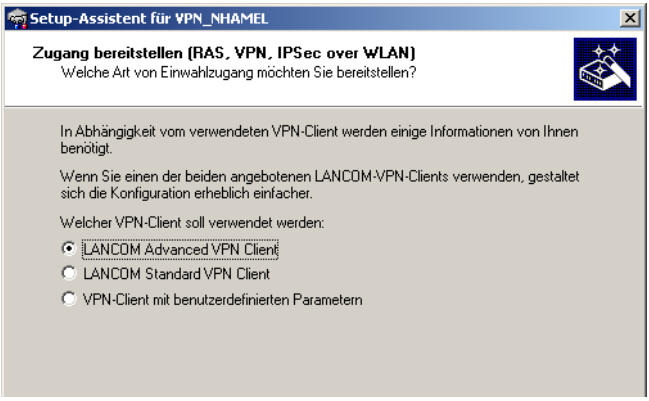
6.2.1 Einwahl über VPN

Für die Einwahl in ein Netzwerk über VPN benötigt ein Rechner:

- Einen Zugang zum Internet
- Einen VPN-Client

LANCOM Systems bietet auf der LANCOM-CD eine 30-Tage-Testversion des LANCOM Advanced VPN Client an. Eine genaue Beschreibung des LANCOM Advanced VPN Client und und Hinweise zur Einrichtung finden Sie ebenfalls auf der CD.

Wählen Sie bei der Konfiguration eines neuen Profils im Konfigurationsassistenten die Option 'LANCOM Advanced VPN Client'.


Setup-Assistent für VPN_NHAMEL
Zugang bereitstellen (RAS, VPN, IPSec over WLAN)
Welche Art von Einwahlzugang möchten Sie bereitstellen?
In Abhängigkeit vom verwendeten VPN-Client werden einige Informationen von Ihnen benötigt.
Wenn Sie einen der beiden angebotenen LANCOM-VPN-Clients verwenden, gestaltet sich die Konfiguration erheblich einfacher.
Welcher VPN-Client soll verwendet werden:
LANCOM Advanced VPN Client
LANCOM Standard VPN Client
VPN-Client mit benutzerdefinierten Parametern

Der Assistent fragt im folgenden die Werte ab, die beim Anlegen des RAS-Zugangs im LANCOM festgelegt wurden.

6.2.2 Einwahl über ISDN

Beim Einwahl-Rechner sind einige Einstellungen nötig, die hier nur kurz am Beispiel eines Windows-Rechners aufgeführt sind:

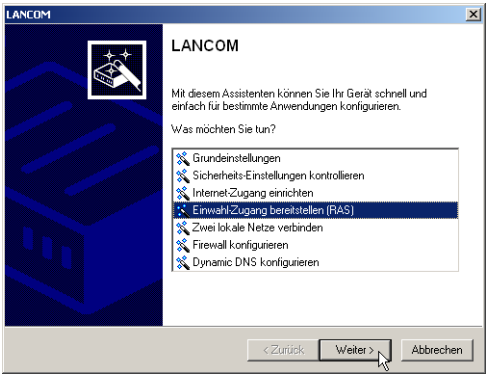
DE

- DFÜ-Netzwerk (bzw. anderer PPP-Client) korrekt eingerichtet
- Netzwerkprotokoll (TCP/IP, IPX) installiert und auf den DFÜ-Adapter gebunden
- neue Verbindung im DFÜ-Netzwerk mit Rufnummer des Routers
- Terminal-Adapter oder ISDN-Karte auf PPPHDLC eingestellt
- PPP als DFÜ-Servertyp ausgewählt, 'Software-Komprimierung aktivieren' und 'Verschlüsseltes Kennwort fordern' ausgeschaltet
- Auswahl der gewünschten Netzwerkprotokolle (TCP/IP, IPX)
- Zusätzliche TCP/IP-Einstellungen:
  - Zuweisung von IP-Adresse und Namensserveradresse aktiviert
  - 'IP-Headerkomprimierung' deaktiviert

Mit diesen Einstellungen kann sich ein PC über ISDN in das entfernte LAN einwählen und in üblicher Weise auf dessen Ressourcen zugreifen.

6.3 Anleitung für LANconfig

① Rufen Sie den Assistenten 'Einwahl-Zugang bereitstellen (RAS)' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.



② Der Assistent meldet, sobald ihm alle notwendigen Angaben vorliegen. Schließen Sie den Assistenten dann mit **Fertig stellen** ab.

③ Konfigurieren Sie wie beschrieben den DFÜ-Netzwerkzugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung' auf Seite 57).

6.4 Anleitung für WEBconfig

① Rufen Sie im Hauptmenü den Assistenten 'Zwei lokale Netze verbinden' auf. Folgen Sie den Anweisungen des Assistenten und geben Sie die notwendigen Daten ein.

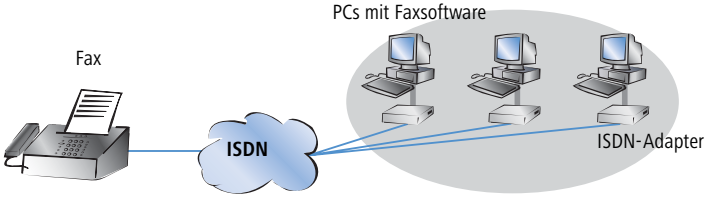
② Konfigurieren Sie wie beschrieben den DFÜ-Netzwerkzugang am Einwahl-PC. Anschließend können Sie die Verbindung testen (siehe Kasten 'Ping – schneller Verbindungstest einer TCP/IP-Verbindung' auf Seite 57).

DE

7 Faxe versenden mit der LANCAPI

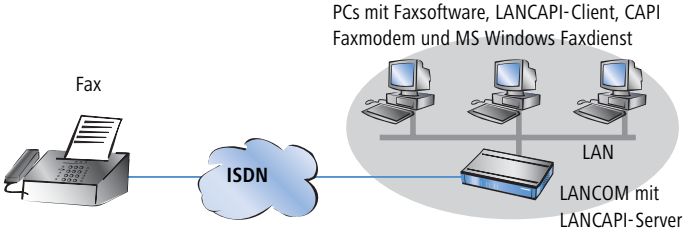
Die LANCAPI von LANCOM ist eine spezielle Form der weit verbreiteten ISDN CAPI-Schnittstelle. CAPI steht für Common ISDN Application Programming Interface und stellt die Verbindung von ISDN-Adaptern zu Kommunikationsprogrammen her. Diese Programme wiederum stellen den Rechnern Funktionen der Bürokommunikation, wie z.B. ein Fax oder einen Anrufbeantworter, bereit.

Der Einsatz der LANCAPI bringt vor allem wirtschaftliche Vorteile. Alle Windows-Arbeitsplätze, die im LAN integriert sind, erhalten über die LANCAPI uneingeschränkten Zugriff auf ISDN-Bürokommunikations-Funktionen wie Fax, Anrufbeantworter, Onlinebanking und Eurofiletransfer. Ohne zusätzliche Hardware an jedem einzelnen Arbeitsplatz werden alle ISDN-Funktionen über das Netzwerk bereitgestellt. Dadurch entfallen kostspielige Ausstattungen der Arbeitsplätze mit ISDN-Adaptern oder Modems. Lediglich die Software für die Bürokommunikation wird auf den einzelnen Arbeitsplätzen installiert.



Mit der LANCAPI von LANCOM können Sie von Ihrem Arbeitsplatzrechner aus bequem Faxe versenden, ohne dass ein Faxgerät angeschlossen ist. Hierzu müssen auf Ihrem Rechner jedoch verschiedene Komponenten installiert sein:

- der **LANCAPI-Client**. Dieser stellt die Verbindung zwischen Ihrem Arbeitsplatzrechner und dem LANCAPI-Server her.
- das **LANCOM CAPI Faxmodem**. Dieses Tool simuliert ein Faxgerät auf Ihrem Arbeitsplatzrechner.
- der **MS-Windows Faxdienst**. Er ist die Schnittstelle zwischen Faxanwendungen und dem virtuellen Fax.



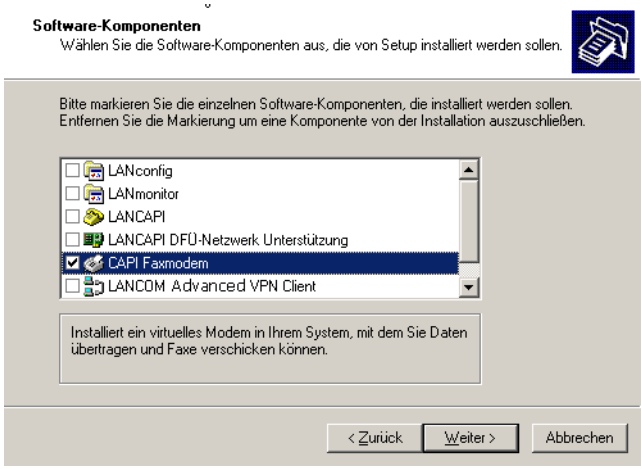
Die Installation des LANCAPI-Clients wird im Referenzhandbuch beschrieben. Dieses Kapitel beschäftigt sich mit der Installation und Konfiguration von LANCOM CAPI Faxmodem und MS-Windows Faxdienst.

7.1 Installation des LANCOM CAPI Faxmodem

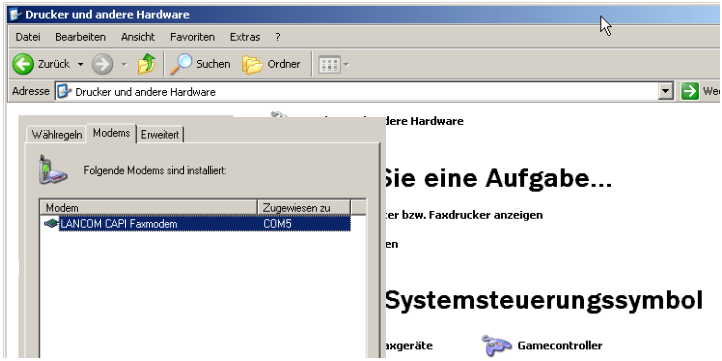
DE

① Wählen Sie im Setup-Programm Ihrer LANCOM-CD den Eintrag **LANCOM Software installieren.**

② Markieren Sie die Option **CAPI Faxmodem**, klicken Sie **Weiter** und folgen Sie den Hinweisen der Installationsroutine**.**


Software-Komponenten
Wählen Sie die Software-Komponenten aus, die von Setup installiert werden sollen.
Bitte markieren Sie die einzelnen Software-Komponenten, die installiert werden sollen.
Entfernen Sie die Markierung um eine Komponente von der Installation auszuschließen.
LANconfig
LANmonitor
LANCAPI
LANCAPI DFÜ-Netzwerk Unterstützung
CAPI Faxmodem
LANCOM Advanced VPN Client
Installiert ein virtuelles Modem in Ihrem System, mit dem Sie Daten übertragen und Faxe verschicken können.
< Zurück
Weiter >
Abbrechen

Ist die Installation erfolgreich verlaufen, ist das LANCOM CAPI Faxmodem in den **Telefon- und Modemoptionen** der Systemsteuerung eingetragen.

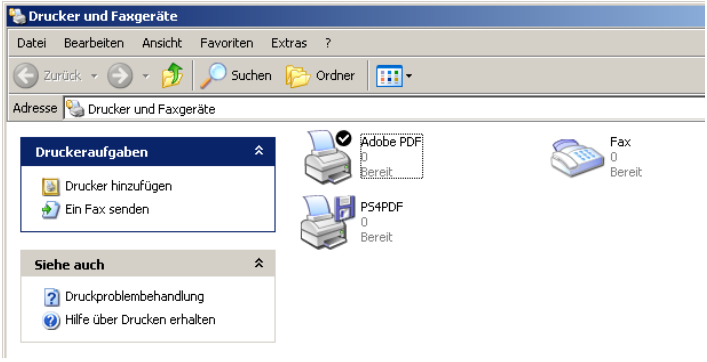


DE

7.2 Installation des MS Windows Faxdienstes

① Wählen Sie in der Systemsteuerung die Option **Drucker und Faxgeräte**.

② Wählen Sie im Fenster Drucker und Faxgeräte die Option **lokalen Faxdrucker installieren**. Folgen Sie ggf. den Anweisungen des Installationstools. In dem aktuellen Fenster erscheint ein Icon für den neu angelegten Faxdrucker.



Zum Überprüfen der Installation klicken sie mit der rechten Maustaste auf das Fax-Icon und wählen **Eigenschaften**. Im Register 'Geräte' sollte das LANCOM CAPI Faxmodem eingetragen sein.

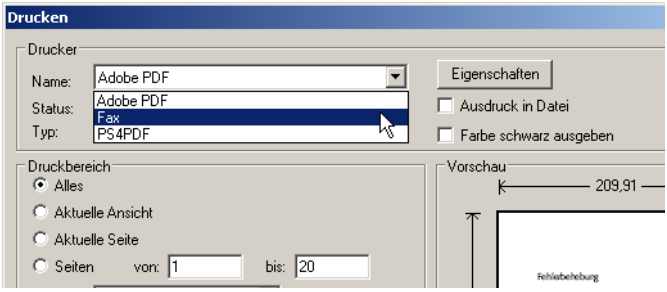
7.3 Versenden eines Faxes

Nachdem alle erforderlichen Komponenten installiert wurden, gibt es mehrere Möglichkeiten, ein Fax von Ihrem Arbeitsplatzrechner aus zu versenden. Haben Sie bereits eine fertige Datei, können Sie diese direkt aus Ihrer jeweiligen Anwendung heraus verschicken. Wollen Sie dagegen nur eine kurze Notiz versenden, wählen sie den MS-Windows Faxdienst. Alternativ können Sie natürlich auch eine beliebige Fax-Software verwenden.

7.3.1 Faxe versenden mit beliebigen Büroanwendungen

① Öffnen Sie wie gewohnt ein Dokument in Ihrer Büroanwendung und wählen Sie den Menüpunkt **Datei/Drucken**.

② Stellen Sie als Drucker das Faxgerät ein.



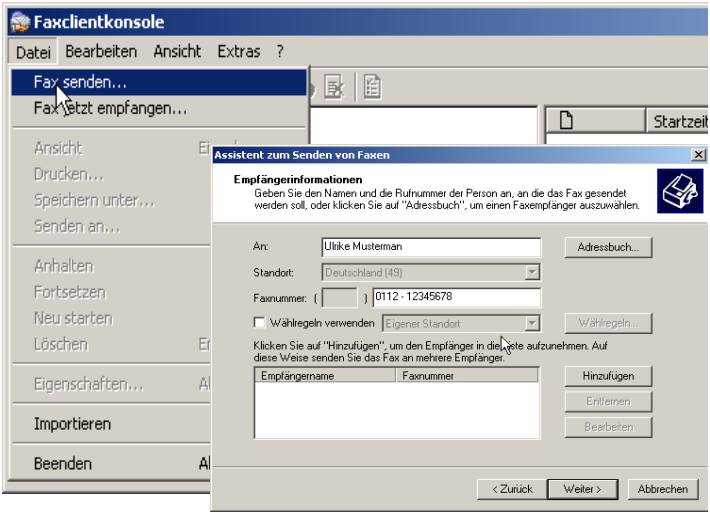
③ Klicken Sie auf OK. Es erscheint ein Assistent, der Sie durch den weiteren Sendevorgang leitet.

7.3.2 Faxe versenden mit dem Windows Faxdienst

① Öffnen Sie in der Systemsteuerung das Fenster **Drucker und Faxgeräte**.

② Doppelklicken Sie mit der linken Maustaste das Icon des Faxgerätes.

③ Es öffnet sich die Faxclientkonsole. Wählen Sie den Menüpunkt **Datei/Fax senden**. Ein Assistent führt sie durch den weiteren Sendevorgang.



DE

8 Sicherheits-Einstellungen

Ihr LANCOM verfügt über zahlreiche Sicherheitsfunktionen. In diesem Kapitel finden Sie alle Informationen, die Sie für eine optimale Absicherung benötigen.

8.1 Der Sicherheits-Assistent

Der Zugriff auf die Konfiguration des Geräts erlaubt nicht nur das Auslesen kritischer Informationen (z. B. WEP-Schlüssel, Internet-Kennwort). Vielmehr können auch die Einstellungen der Sicherheitsfunktionen (z. B. Firewall) nach Belieben geändert werden. Dadurch bringt der unbefugter Konfigurationszugriff nicht nur das einzelne Gerät, sondern das gesamte Netzwerk in große Gefahr.

Ihr LANCOM verfügt über einen Kennwortschutz für den Konfigurationszugang. Dieser wird schon während der Grundkonfiguration durch Angabe eines Kennwortes aktiviert.

Das Gerät sperrt den Konfigurationszugang automatisch für eine festgelegte Dauer, wenn eine bestimmte Anzahl von Anmelde-Fehlversuchen feststellt wird. Sowohl die kritische Anzahl Fehlerversuche als auch die Dauer der Sperre lassen sich modifizieren. Standardmäßig sperrt das Gerät nach dem fünften Fehlerversuch für eine Dauer von fünf Minuten.

Neben diesen grundlegenden Einstellungen prüfen Sie mit dem Sicherheitsassistenten auch die Sicherheitseinstellungen für das Funknetzwerk, sofern Ihr Gerät über eine WLAN-Schnittstelle verfügt.

8.1.1 Assistent für LANconfig

① Markieren Sie Ihr LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras** ▶ **Setup Assistent**.

② Wählen Sie im Auswahlmenü den Setup-Assistenten **Sicherheitseinstellungen kontrollieren** und bestätigen Sie die Auswahl mit **Weiter**.

③ In den folgenden Fenstern stellen Sie das Passwort ein und wählen die zulässigen Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerken aus. Zusätzlich stellen Sie die MSN für die Fernkonfiguration über ISDN ein.

④ In einem weiteren Schritt werden die Parameter der Konfigurationssperre wie Anzahl der Fehllogins und Dauer der Sperre eingestellt.

⑤ Im Bereich der Firewall aktivieren Sie die Stateful-Inspection, das Ping-Blocking und den Stealth-Mode.

⑥ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

8.1.2 Assistent für WEBconfig

Unter WEBconfig besteht die Möglichkeit, den Assistenten **Sicherheitseinstellungen** aufzurufen und die Einstellungen zu kontrollieren und zu ändern. Dabei werden die folgenden Werte bearbeitet:

- Passwort für das Gerät
- zulässige Protokolle für den Konfigurationszugriff von lokalen und entfernten Netzwerke
- die MSN für die Fernkonfiguration über ISDN
- Parameter der Konfigurationssperre (Anzahl der Fehllogins und Dauer der Sperre)

8.2 Der Firewall-Assistent

Der LANCOM verfügt über eine Stateful-Inspection-Firewall und Firewall-Filter zur wirksamen Absicherung Ihres WLANs gegenüber dem Internet. Kernidee der Stateful-Inspection-Firewall ist, dass nur selbstinitiierter Datentransfer als zulässig betrachtet wird. Alle Zugriffe, die unaufgefordert nicht aus dem lokalen Netz heraus erfolgen, sind unzulässig.

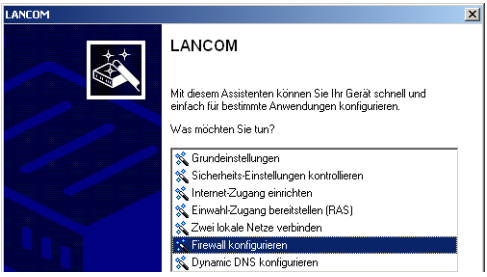
Der Firewall-Assistent hilft Ihnen, schnell und komfortabel neue Regeln für die Firewall zu erstellen.

Nähere Informationen zur Firewall Ihres LANCOM und zu deren Konfiguration finden Sie im Referenzmanual.

DE

8.2.1 Assistent für LANconfig

① Markieren Sie Ihr LANCOM im Auswahlfenster. Wählen Sie aus der Befehlsleiste den Punkt **Extras ▶ Setup Assistent**.



② Wählen Sie im Auswahlmenü den Setup-Assistenten **Firewall konfigurieren** und bestätigen Sie die Auswahl mit **Weiter**.

③ In den folgenden Fenstern wählen Sie aus, auf welche Dienste/Protokolle sich die Regel bezieht. Im nächsten Schritt legen Sie fest, für welche Quell- und Zielstationen die Regel gilt und welche Aktionen ausgeführt werden sollen, wenn die Regel auf ein Datenpaket zutrifft.

④ Zum Abschluss geben Sie der neuen Regel einen Namen, aktivieren sie und legen fest, ob weitere Regeln beachtet werden sollen, wenn die Regel auf ein Datenpaket zutrifft.

⑤ Der Assistent informiert Sie sobald die Eingaben vollständig sind. Schließen Sie die Konfiguration mit **Fertig stellen** ab.

8.2.2 Konfiguration unter WEBconfig

Unter WEBconfig besteht die Möglichkeit, die Parameter zur Absicherung des Internet Zugriffs unter **Konfiguration ▶ Firewall / QoS ▶ Regeln ▶ Regeltabelle** aufzurufen, die Einstellungen zu kontrollieren und zu ändern.

8.3 Die Sicherheits-Checkliste

In der folgenden Checkliste finden Profis alle wichtigen Sicherheitseinstellungen im Überblick. Die meisten Punkte dieser Checkliste sind in einfachen Konfigurationen unbedenklich. In solchen Fällen reichen die Sicherheitseinstellungen aus, die während der Grundkonfiguration oder mit dem Sicherheits-Assistenten gesetzt werden.

Detaillierte Informationen zu den angesprochenen Sicherheitseinstellungen finden Sie im Referenzhandbuch.

- **Haben Sie ein Kennwort für die Konfiguration vergeben?**

  Die einfachste Möglichkeit zum Schutz der Konfiguration ist die Vereinbarung eines Kennworts. Solange Sie kein Kennwort vereinbart haben, kann jeder die Konfiguration des Gerätes verändern. Das Feld zur Eingabe des Kennworts finden Sie in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Es ist insbesondere dann unerlässlich, ein Kennwort zur Konfiguration zu vergeben, wenn Sie die Fernkonfiguration erlauben wollen!

- **Haben Sie die Fernkonfiguration zugelassen?**

  Wenn Sie die Fernkonfiguration nicht benötigen, so schalten Sie sie ab. Wenn Sie die Fernkonfiguration benötigen, so vergeben Sie unbedingt einen Kennwortschutz für die Konfiguration (siehe vorhergehender Abschnitt). Das Feld zur Abschaltung der Fernkonfiguration finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'. Wählen Sie hier unter 'Zugriffsrechte - von entfernten Netzen' für alle Konfigurationsarten die Option 'nicht erlaubt'

- **Haben Sie die SNMP-Konfiguration mit einem Kennwort versehen?**

  Schützen Sie auch die SNMP-Konfiguration mit einem Kennwort. Das Feld zum Schutz der SNMP-Konfiguration mit einem Kennwort finden Sie ebenfalls in LANconfig im Konfigurationsbereich 'Management' auf der Registerkarte 'Security'.

- **Haben Sie die Firewall aktiviert?**

  Die Stateful-Inspection Firewall der LANCOM Router sorgt dafür, dass Ihr lokales Netzwerk von außen nicht angegriffen werden kann. Die Firewall können Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Allgemein' einschalten.

- **Verwenden Sie eine 'Deny-All' Firewall-Strategie?**

  Für maximale Sicherheit und Kontrolle unterbinden Sie zunächst jeglichen Datentransfer durch die Firewall. Nur die Verbindungen, die explizit gestattet sein sollen, sind in die Firewall einzutragen. Damit wird 'Trojanern' und bestimmten E-Mail-Viren der Kommunikations-Rückweg entzogen. Die Firewall-Regeln finden Sie in LANconfig unter 'Firewall/Qos' auf der Registerkarte 'Regeln' zusammengefasst. Eine Anleitung dazu fin-

det sich unter "Aufbau einer expliziten "Deny-All"-Strategie" on page 156.

- **Haben Sie IP-Masquerading aktiviert?**

  IP-Masquerading heißt das Versteck für alle lokalen Rechner beim Zugang ins Internet. Dabei wird nur das Router-Modul des Geräts mit seiner IP-Adresse im Internet bekannt gemacht. Die IP-Adresse kann fest vergeben sein oder vom Provider dynamisch zugewiesen werden. Die Rechner im LAN nutzen den Router dann als Gateway und können selbst nicht erkannt werden. Der Router trennt Internet und Intranet wie eine Wand. Die Verwendung von IP-Masquerading wird für jede Route in der Routing-Tabelle einzeln festgelegt. Die Routing-Tabelle finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Router'.

- **Haben Sie kritische Ports über Filter geschlossen?**

  Die Firewall-Filter des LANCOM bieten Filterfunktionen für einzelne Rechner oder ganze Netze. Es ist möglich, Quell- und Ziel-Filter für einzelne Ports oder auch Portbereiche aufzusetzen. Zudem können einzelne Protokolle oder beliebige Protokollkombinationen (TCP/UDP/ICMP) gefiltert werden. Besonders komfortabel ist die Einrichtung der Filter mit Hilfe von LANconfig. Unter 'Firewall/QoS' finden Sie die Karteikarte 'Regeln', mit deren Hilfe Filterregeln definiert und verändert werden können.

- **Haben Sie bestimmte Stationen von dem Zugriff auf den Router ausgeschlossen?**

  Mit einer speziellen Filter-Liste kann der Zugriff auf die internen Funktionen der Geräte über TCP/IP eingeschränkt werden. Mit den internen Funktionen werden hierbei Konfigurationssitzungen über LANconfig, WEBconfig, Telnet oder TFTP bezeichnet. Standardmäßig enthält diese Tabelle keine Einträge, damit kann also von Rechnern mit beliebigen IP-Adressen aus über TCP/IP mit Telnet oder TFTP ein Zugriff auf den Router gestartet werden. Mit dem ersten Eintrag einer IP-Adresse sowie der zugehörigen Netzmaske wird der Filter aktiviert, und nur noch die in diesem Eintrag enthaltenen IP-Adressen werden berechtigt, die internen Funktionen zu nutzen. Mit weiteren Einträgen kann der Kreis der Berechtigten erweitert werden. Die Filter-Einträge können sowohl einzelne Rechner als auch ganze Netze bezeichnen. Die Zugangsliste finden Sie in LANconfig im Konfigurationsbereich 'TCP/IP' auf der Registerkarte 'Allgemein'.

- **Lagern Sie Ihre abgespeicherte LANCOM-Konfiguration an einem sicheren Ort?**

  Schützen Sie abgespeicherte Konfigurationen an einem sicheren Ort vor unberechtigtem Zugriff. Eine abgespeicherte Konfiguration könnte sonst von einer unberechtigten Person in ein anderes Gerät geladen werden, wodurch z. B. Ihre Internet-Zugänge auf Ihre Kosten benutzt werden können.

9 Rat & Hilfe

In diesem Kapitel finden Sie Ratschläge und Hilfestellungen für die erste Hilfe bei einigen typischen Problemen.

9.1 Es wird keine WAN-Verbindung aufgebaut

Nach dem Start versucht der Router automatisch, Kontakt zum Zugangsanbieter aufzunehmen. Während dieser Phase blinkt die Online-LED grün. Im Erfolgsfall wechselt diese LED dann auf dauerhaftes Grün mit kurzen Unterbrechungen. Schlägt die Kontaktaufnahme hingegen fehl, so leuchtet die Online-LED rot. In der Regel ist eine der folgenden Ursachen:

Probleme an der Verkabelung?

Verwenden Sie für den WAN-Anschluss ausschließlich das mitgelieferte Anschlusskabel. Dieses Kabel muss mit dem Ethernet-Ausgang des Netzabschlusses verbunden sein. Die WAN-Link-LED muss zum Zeichen der physikalischen Verbindung grün leuchten.

Stimmt das gewählte Übertragungsprotokoll?

Das Übertragungsprotokoll wird bei der Grundeinstellung gesetzt. Dabei setzt der Grundeinstellungs-Assistent für zahlreiche DSL-Anbieter selbstständig das korrekte Übertragungsprotokoll. Nur wenn Ihr DSL-Anbieter dem Assistenten unbekannt ist, müssen Sie das verwendete Protokoll selber angeben. In jedem Fall sollte das Protokoll funktionieren, das Ihnen Ihr DSL-Anbieter angibt.

Die Protokoll-Einstellung kontrollieren und korrigieren Sie unter:

Konfigurationstool	Aufruf
LANconfig	Management ▶ Interfaces ▶ Interface-Einstellungen ▶ WAN-Interface
WEBconfig	Experten-Konfiguration ▶ Setup ▶ Interface ▶ WAN-Interface

9.2 DSL-Übertragung langsam

Die Übertragungsgeschwindigkeit einer (Internet-) DSL-Verbindung hängt von zahlreichen Faktoren ab, von denen die meisten außerhalb des eigenen

Einflussbereiches liegen: Entscheidend sind neben der Bandbreite der eigenen Internet-Anbindung beispielsweise auch die Internet-Anbindung und Auslastung des angesprochenen Ziels. Außerdem können zahlreiche Faktoren im Internet die Übertragungsleistung beeinflussen.

Vergrößerung der TCP/IP-Windows-Size unter Windows

Wenn die tatsächliche Übertragungsleistung einer DSL-Verbindung deutlich unter den vom DSL-Anbieter angegebenen Maximalwerten liegt, gibt es außer diesen externen Einflussfaktoren nur wenige mögliche Fehlerquellen an den eigenen Geräten.

Ein übliches Problem tritt auf, wenn an einem Windows-PC über eine asynchrone Verbindung gleichzeitig große Datenmengen geladen und gesendet werden. In diesem Fall kann es zu einer starken Beeinträchtigung der Download-Geschwindigkeit kommen. Verantwortlich ist die sogenannte TCP/IP-Receive-Windows-Size im Windows-Betriebssystem, die standardmäßig auf einen für asynchrone Verbindungen zu kleinen Wert gesetzt ist.

Eine Anleitung zur Vergrößerung der Windows-Size finden Sie in der Wissensdatenbank im Support-Bereich der LANCOM-Website (www.lancom.de).

9.3 Unerwünschte Verbindungen mit Windows XP

Windows-XP-Rechner versuchen beim Start, die eigene Uhrzeit mit einem Zeitserver im Internet abzugleichen. Deshalb kommt es beim Start eines Windows-XP-Rechners im WLAN zum Verbindungsaufbau des LANCOM mit dem Internet.

Zur Abhilfe schaltet man an den Windows-XP-Rechnern die automatische Zeitsynchronisation unter **Rechter Mausklick auf die Uhrzeit ▶ Eigenschaften ▶ Internetzeit** aus.

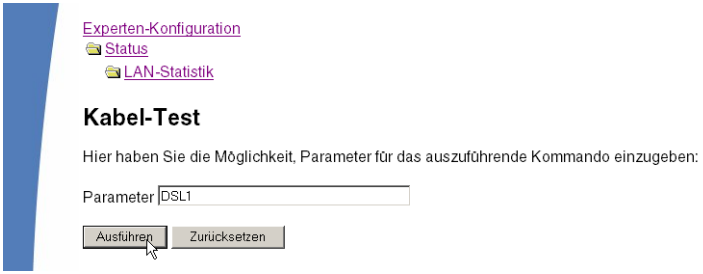
9.4 Kabel testen

Nur LANCOM 1711 VPN

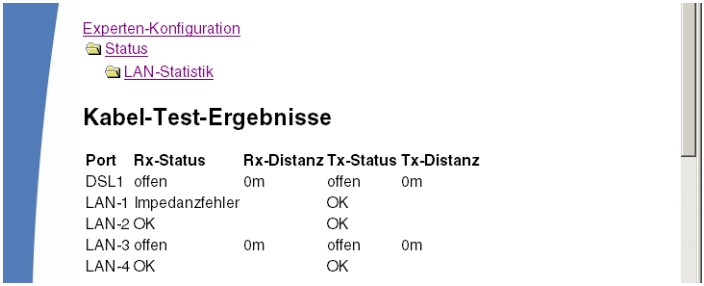
Werden auf Ihren LAN- oder WAN-Verbindungen gar keine Daten übertragen, obwohl die Konfiguration der Geräte keine erkennbaren Fehler aufweist, liegt möglicherweise ein Defekt in der Verkabelung vor.

Mit dem Kabel-Test können Sie aus dem LANCOM heraus die Verkabelung testen. Wechseln Sie dazu unter WEBconfig in den Menüpunkt **Expertenkonfiguration ▶ Status ▶ LAN-Statistik ▶ Kabel-Test**. Geben Sie dort die Bezeichnung des Interfaces ein, das Sie testen wollen (z.B. "DSL1" oder "LAN-1"). Achten Sie dabei auf die genaue Schreibweise der Interfaces. Mit einem

Klick auf die Schaltfläche **Ausführen** starten Sie den Test für das eingetragene Interface.



Wechseln Sie anschließend in den Menüpunkt **Expertenkonfiguration** ▶ **Status** ▶ **LAN-Statistik** ▶ **Kabel-Test-Ergebnisse**. In der Liste sehen Sie die Ergebnisse, die der Kabel-Test für die einzelnen Interfaces ergeben hat.



Als Ergebnisse können folgende Werte erscheinen:

- **OK**: Kabel richtig eingesteckt, Leitung in Ordnung.
- **offen** mit Distanz **"0m"**: kein Kabel eingesteckt oder eine Unterbrechung in weniger als ca. 10 Metern.
- **offen** mit Angabe einer konkreten Distanz: Kabel ist eingesteckt, hat jedoch in der angegebenen Entfernung einen Defekt (Kurzschluss).
- **Impedanzfehler**: Das Kabelpaar am anderen Ende ist nicht mit der korrekten Impedanz abgeschlossen.

10 Anhang

10.1 Leistungs- und Kenndaten

		LANCOM 821 ADSL/ISDN	LANCOM 1621 ADSL/ISDN	LANCOM 1711 VPN
Anschlüsse	Ethernet LAN	4 x RJ-45 Ethernet IEEE 802.3 (Switch), 10/100Base-T-Autosensing, Node/Hub-Autodetection		
		Alle Ports können gemeinsam in den 'Private Mode' geschaltet werden. In diesem Modus sind die Ports untereinander abgeschirmt.		Einzelne Ports können individuell in den 'Private-Mode' geschaltet werden, z.B. als DMZ-Port
				Cable Tester zur Überprüfung der Verkabelung
	WAN bzw. ADSL	'Annex A'-Geräte: ADSL over POTS nach ITU G.992.1 Annex A, ANSI T1.413, ITU G.992.2 (G.Lite), G.994.1 (G.hs); 'Annex B'-Geräte: ADSL over ISDN nach ITU G.992.1 Annex B, sowie ADSL over ISDN proprietär (Texas Instruments, ADI, Alcatel), ETSI TS 101 388;		10/100Base-TX, Autosensing
	DSLoL (DSL over LAN)	LANCOM 821 ADSL/ISDN und LANCOM 1621 ADSL/ISDN können zusätzlich einen freien Switch-Port als WAN-Zugang benutzen (DSLoL-Schnittstelle). Das kann z.B. zum späteren Upgrade auf einen SDSL-Anschluss genutzt werden. Am DSLoL-Anschluss funktioniert entweder ein Modem (nur für PPPoE-basierte Zugänge), oder aber ein Netzabschlussrouter (mit statischer IP-Adresse).		
	ISDN	ISDN S_0		
	Outband	serieller V.24/V.28-Port (8-pol. Mini-DIN)		
	Stromversorgung	12V über externes Netzteil		
Betriebsarten	Multiprotokoll-Router	IP-Router, IPX-Router, NAT/Reverse NAT (IP-Masquerading) DHCP-Server inkl. Autodetection, DHCP-Client, DHCP-Relay-Server, DNS-Server, PPPoE-Client, PPTP-Client, NetBIOS-Proxy, DynDNS-Client, N:N-Mapping (nur LANCOM 1621 ADSL/ISDN und LANCOM 1711 VPN)		
	ISDN Gateway	ISDN-S0-Bus, Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Konfiguration, I.430, (Autosensing); D-Kanal: 1TR6, DSS1 (Euro-ISDN); B-Kanal: PPP (asynchron/synchron), X.75, HDLC, MLPPP für Kanalbündelung, CAPI 2.0 über LANcapi, Stac-Datenkompression		

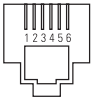
		LANCOM 821 ADSL/ISDN	LANCOM 1621 ADSL/ISDN	LANCOM 1711 VPN
Protokolle	LAN	IP: ARP, Proxy ARP, IP, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS, SNMP, HTTP, HTTPS, BOOTP, NTP, NetBIOS, LANCAPI		
		IPX: RIP, SAP, IPX- und SPX-Watchdogs, NetBIOS Watchdogs		
	WAN	PPPoE, PPPoA, PPTP, IPoA und Plain Ethernet		
Übertragungsraten (maximum)	LAN	100 Mbit/s, Vollduplex-Betrieb		
	WAN	Downstream 8 Mbit/s, upstream 800 kbit/s		
ATM	Transport	Bis zu 8 ATM AAL-5 PVCs		
	OAM	ATM-F4- und F5-Loop-Back		
Sicherheit		Intrusion-Detection (IP-Spoofing, Login-Versuche, Portscans), Denial-of-Service Protection (Fragmentierungsfehler, SYNFlooding, automatisches Schließen von Ports/Verbindungen). DNS-Hitlisten sowie Wildcard-Filter (URL-Blocking). Hochverfügbarkeit durch ISDN Dial-Backup für Internetzugang. Alarmierung durch Email, SNMP-Traps und SYSLOG. PAP, CHAP und MS-CHAP als PPP-Authentifizierungsmechanismen, passwortgeschützter Konfigurationszugang pro Interface, Access-Control-Liste (IP-, MAC- und Protokollfilter) für Konfigurationszugang und LANCAPI, ISDN-Einwahlnummernliste. FirmSafe mit 2 Firmware-Versionen für absolut sichere Software-Upgrades.		
Firewall	Stateful-Inspection, IP-Paketfilter mit Port-Bereichen; Maskierung (NAT/PAT) von TCP, UDP, ICMP, FTP, PPTP, H.323,Net-Meeting, IRC und IPSec; DNS-Forwarding; inverse Maskierung für IP-Dienste aus dem Intranet wie z.B. Web-Server; Unterstützung von 2 lokalen Netzen (LAN plus DMZ); DMZ mit eigenem IP-Adresskreis ohne NAT; IP-QoS und Bandbreitenmanagement / Priorisierung, z.B. für VoIP			
Management	LANtools (Professionelle Management-Software für Windows), WEBconfig (HTTP / HTTPS), Telnet, TFTP, SNMP V2 (MIB II, 802.11, 802.1D, 802.3, Private MIB), RADIUS, Syslog Fernwartung über ISDN, DynDNS Outband-Schnittstelle: Kommandozeilen-Interface			
Gehäuse		210 x 143 x 45 mm (B x H x T), robustes Kunststoffgehäuse, Anschlüsse auf der Rückseite, stapelbar, für Wandmontage vorbereitet		
Normen		EU (CE-Zertifizierung: EN 55022, EN 55024, EN 60950)		
				Getestet und freigegeben für den Einsatz im medizinischen Umfeld nach EN60601-1-2.
Umgebung / Temperatur		5 °C bis +40 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend)		5 °C bis +55 °C bei 80% max. Luftfeuchtigkeit (nicht kondensierend)

		LANCOM 821 ADSL/ISDN	LANCOM 1621 ADSL/ISDN	LANCOM 1711 VPN
Optionen		LANCOM Festverbindungsoption (Art.Nr. 00789)		
		LANCOM Service-Option (4 Jahre Garantie, Vorabaustausch) (Art.-Nr. 61401)		
			LANCOM VPN Option 25 Kanäle (Maximal 25 gleichzeitige Verbindungen, 50 Verbindungen konfigurierbar) für VPN im WAN (Art.-Nr. 60083)	LANCOM VPN Option 25 Kanäle (hardwarebeschleunigt, maximal 25 gleichzeitige Verbindungen, 50 Verbindungen konfigurierbar) für VPN im WAN (Art.-Nr. 60083)

10.2 Anschlussbelegung

10.2.1 ADSL-Schnittstelle

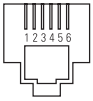
6-polige RJ45-Buchse

Steckverbindung	Pin	IAE
	1	–
	2	–
	3	a
	4	b
	5	–
	6	–

DE

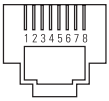
10.2.2 Ethernet WAN-Schnittstelle (LANCOM 1711 VPN)

6-polige RJ45-Buchse

Steckverbindung	Pin	IAE
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-

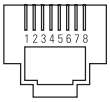
10.2.3 ISDN-S_0-Schnittstelle

8-polige RJ45-Buchse, entsprechend ISO 8877, EN 60603-7

Steckverbindung	Pin	Leitung	IAE
	1	–	–
	2	–	–
	3	T+	2a
	4	R+	1a
	5	R-	1b
	6	T-	2b
	7	–	–
	8	–	–

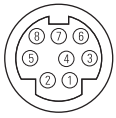
10.2.4 Ethernet-Schnittstellen 10/100Base-T

8-polige RJ45-Buchsen, entsprechend ISO 8877, EN 60603-7

Steckverbindung	Pin	Leitung
	1	T+
	2	T-
	3	R+
	4	–
	5	–
	6	R-
	7	–
	8	–

10.2.5 Konfigurationsschnittstelle (Outband)

8-polige Mini-DIN-Buchse

Steckverbindung	Pin	Leitung
	1	CTS
	2	RTS
	3	RxD
	4	RI
	5	TxD
	6	DSR
	7	DCD
	8	DTR
	U	GND

10.3 CE-Konformitätserklärungen

Die CE-Konformitätserklärungen für LANCOM-Router finden Sie im Download-Bereich der LANCOM-Website (www.lancom.de).

11 Index

Numerics

10/100Base-TX 29
3-DES 50, 59

A

Accounting 37
ADSL 26
  Anschluss 29
  Übertragungsraten 10, 80
ADSL over ISDN 12, 79
ADSL over POTS 12, 79
ADSL-Anschlusskabel 22
AES 50, 59
Amtsvorwahl 37, 44
Annex A 12
Annex B 12
Anrufbeantworter 10
Anschlussbelegung 81
  ADSL-Schnittstelle 81
  Ethernet-Schnittstelle 83
  ISDN-S0-Schnittstelle 82
  Konfigurationsschnittstelle 83
  LAN-Schnittstelle 83
  Outband 83
  WAN-Schnittstelle 83
ATM 80
  Parameter für Internet-Zugang 46
Autosensing 30

B

Blowfish 50, 59

C

Calling Line Identity (CLI) 61
CAPI-Schnittstelle 66
Common ISDN Application Programming Interface (CAPI) 66

D

Datenfrequenzen 10
Default-Gateway 74
Denial-of-Service Protecion 16
DFÜ-Adapter 64
DHCP 44
  DHCP-Server 19, 35, 36, 38, 42, 44
DNS
  DNS-Server 19, 44
  Zugriffe ins entfernte LAN 54
Dokumentation 22
Domäne 54
Download 4
Downstream 10
DSL-Anbieter 39, 43
DSL-Technologien 10
DSL-Übertragung zu langsam 76
DSL-Übertragungsprotokoll 39, 43

E

Einwahl-Zugang 59
Encapsulation 46

F

Fax 10
Fernkonfiguration 38, 43
Fernkonfiguration über ISDN 21
Fernkonfigurationszugang 36
Filtermechanismen 19
Firewall 15, 20, 74
  Stationen sperren 74
Firewall-Filter 71
FirmSafe 21
Firmware 4
Flatrate 47

G

Gebührenbudget 37
Gebührenimpuls 37
Gebühreninformationen 44
Gebührenschutz 37, 39, 43

Gebührenschutz zurücksetzen 25
Gebührensperre 25
Grundkonfiguration 34

H

Hardware-Installation 30
Hinweis-Symbole 5

I

ICMP 74
Installation 22
  ADSL 30
  DSL 30
  ISDN 30
  Konfigurations-Schnittstelle 30
  LAN 30
  LANtools 31
  Netzteil 31
Internet-Anbieter 46
Internet-Zugang 18, 19, 46
  Authentifizierungsdaten 46
  Default-Gateway 47
  DNS-Server 47
  Flatrate 47
  IP-Adresse 47
  Netzmaske 47
  Protokoll 46, 47
Intrusion Detection 16
IP
  Filter 74
  Ports sperren 74
IP-Adresse 30, 35, 36, 55, 74
IP-Masquerading 15, 18, 20, 74
IPoA 46
IPoE 47
IPoEoA 47
IP-Router 19
IPSec 50, 59
IPX 64
  Binding 56, 62
  External Network Number 55, 62
  Frame-Typs 56
  Internal-Net-Number 62
IPX-Konventionen 55
IPX-Router 19
  Einstellungen 55
ISDN 18
  Anschlusskabel 22
  D-Kanal 61
  dynamische Kanalbündelung 47
  Einwahlnummer 47
  Gebühreninformationen 39
  Grundkonfiguration 44
  MSN 36, 39, 44
  NTBA 31
  S0-Anschluss 29
ISDN Kanal 27
ISDN-Anruferkennung 53, 60, 61
ISDN-Anschluss 31
  Grundeinstellungen 36
ISDN-Datenkompression 48
ISDN-Festverbindungsoption 21
ISDN-Modem 59
ISDN-Rufnummer 52
ISDN-S0-Anschluss 20
ISDN-Telefonanlage 37

K

Kennwort 36, 38, 50, 59
Kennwort für die ISDN-Verbindung 53
Konfigurationsdatei 75
Konfigurationskennwort 73
Konfigurations-Schnittstelle 21
  Anschlusskabel 22
Konfigurationsschnittstelle 29
Konfigurationsschutz 20, 36
Konfigurationszugriff 39, 43
Konformitätserklärungen 83

L

LAN
  Anschlusskabel 22

DE

DE

LANCAPI 20, 37
Systemvoraussetzungen 23
LANCOM Online Dokumentation 33
LANCOM-Setup 32
LANconfig 32, 37
Assistenten aufrufen 48
LAN-LAN-Kopplung 18, 19, 36, 50
erforderliche Angaben 51
LANmonitor 32
LANtools
Systemvoraussetzungen 23
Lieferumfang 22
Line-Management 18
LLC-based Multiplexing 46

M

MAC-Adressfilter 15, 20
Mindestbandbreite 16
MSN 61
Multimode 39, 43

N

NAT – siehe IP-Masquerading
Nebenstellenanlage 10
NetBIOS 56
NetBIOS-Proxy 19
Netzmaske 35, 36, 74
Netzschalter 29
Netzteil 22, 29
Netzwerkkopplung 50
Sicherheitsaspekte 50, 59
Netzwerksegment 30, 55
Neustart des Geräts 29

P

PAT – siehe IP-Masquerading
Ping 57
Plain Ethernet 46, 47
Plain IP 46, 47
POTS 12
PPP 59
PPP-Client 64
PPPoA 46
PPPoE 46, 47
PPTP 47

Q

Quality-of-Service 16

R

RAS 13, 15
Remote Access Service (RAS)
Funktion 19
MSN angeben 37
Remote-Access-Service (RAS)
Benutzername 60
einrichten 59
Einwahl-Rechner konfigurieren 63
IPX 62
NetBIOS 62
Server 19
Software-Komprimierung aktivieren 64
TCP/IP 61
Windows-Arbeitsgruppe suchen 62
Reset-Schalter 29
Router 17
Routerfunktion 9
Routing-Tabelle 74
Rückruf 19
Rückruf-Funktion 21
Rückruffunktion 50, 59

S

Sicherheits 70
Sicherheits-Checkliste 72
Sicherheits-Einstellungen 70, 76
Sicherheitseinstellungen 3
Sicherheitsfunktionen 18
SNMP
Konfiguration schützen 73
Software-Installation 31
Splitter 10, 31

Sprachfrequenzen 10
Standard-Gateway 44
Stateful-Inspection 15
Stateful-Inspection-Firewall 71
Statusanzeigen 23
  LAN 28
  Online 26
  Power 24, 25
Support 4
Switch 29
Systemvoraussetzungen 22

T
TAE-Dose 31
TCP 74
TCP/IP 23, 64
  Einstellungen 34, 38, 42
  Einstellungen an den PCs im LAN 44
  Verbindung testen 57
TCP/IP-Filter 15, 20, 74
TCP/IP-Konfiguration
  automatisch 42
  manuell 34, 36
  vollautomatisch 34, 35
TCP/IP-Router
  Einstellungen 53
TCP/IP-Windows-Size 77
T-DSL 12
Telefon 10
Telnet 74
TFTP 74

U
Übertragungsprotokoll 76
UDP 74
Upstream 10

V
VC-based Multiplexing 46
Verschlüsselung 50, 59
Virtual Circuit Identifier (VCI) 46
Virtual Path Identifier (VPI) 46
Virtual Private Network 12
Virtual Private Network (VPN) 18, 19
VPN 12
VPN-Client 63

W
WAN
  Anschlusskabel 22
WAN-Anschluss 29
WAN-Verbindung
  Probleme beim Aufbau 76
WEBconfig 39
  Aufruf eines Assistenten 41
  Kennworteingabe 43